IMPLEMENTACIÓN DE UN SISTEMA INALÁMBRICO EN COMUNICACIONES DE DATOS PARA LAS DIFERENTES UNIVERSIDADES

LEONARDO STEVENSON HERNÁNDEZ

YENIS SANTANDER PALMERA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
CARTAGENA
2005

IMPLEMENTACIÓN DE UN SISTEMA INALÁMBRICO EN COMUNICACIONES DE DATOS PARA LAS DIFERENTES UNIVERSIDADES

LEONARDO STEVENSON HERNANDEZ

YENIS SANTANDER PALMERA

Trabajo de Monografía presentado como requisito para optar al título de Ingeniero Electrónico

Director:

JOSÉ BARBA MERCADO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERIA ELÉCTRICA Y ELECTRONICA

CARTAGENA de Indias, D.T. y C. junio 2005

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Cartagena de Indias, D.T. y C., Junio 2005

Señores:

Departamento de Investigaciones

Universidad Tecnológica De Bolívar

Cartagena de Indias, D.T. y C.

Respetados Señores:

Presento para su consideración el Proyecto de Monografía titulado: **IMPLEMENTACIÓN DE UN SISTEMA INALÁMBRICO EN COMUNICACIONES DE DATOS PARA LAS DIFERENTES UNIVERSIDADES,** como requisito para optar el titulo de ingeniero electrónico

Atentamente,

_____

LEONARDO STEVENSON HERNANDEZ

Cartagena de Indias, D.T. y C., Junio 2005.

Señores:
Departamento de Investigaciones
Universidad Tecnológica De Bolívar
Cartagena de Indias, D.T. y C.

Respetados Señores:

Presento para su consideración el Proyecto de Monografía titulado: **IMPLEMENTACIÓN DE UN SISTEMA INALÁMBRICO EN COMUNICACIONES DE DATOS PARA LAS DIFERENTES UNIVERSIDADES,** como requisito para optar el título de Ingeniero Electrónico.

Atentamente,

_____

YENIS SANTANDER PALMERA

Cartagena de Indias, D.T. y C., Junio 2005

Señores

Departamento De Investigaciones

Universidad Tecnológica de Bolívar

Cartagena de Indias, D.T. y C.

Respetado Señores:

Por solicitud de los estudiantes LEONARDO STEVENSON HERNANDEZ Y YENNIS SANTANDER, dirigí a satisfacción el proyecto de monografía titulado: **IMPLEMENTACIÓN DE UN SISTEMA INALÁMBRICO EN COMUNICACIONES DE DATOS PARA LAS DIFERENTES UNIVERSIDADES**, como requisito para optar al titulo de Ingeniero Electrónico.

Espero que el contenido y las normas aplicadas cumplan con los requisitos exigidos por esta dirección.

Atentamente,

_____

JOSE BARBA MERCADO

AGRADECIMIENTOS

Agradezco a DIOS padre todo poderoso que me dio la fuerza necesaria para alcanzar este gran logro, y me brindo coraje para sortear los diferentes obstáculos que se presentaron en este camino.

A mi madre NELCY HERNÁNDEZ VILLADIEGO, quien fue mi estimulo en esta gran lucha, y la que con su empuje y temple me brindo todo el apoyo necesario en los momentos de alegría y tristeza.

A mi padre OSWALDO STEVENSON GONZÁLES, quien DIOS lo tenga en su sano reino, quien confió en mí para comenzar esta ardua tarea, y que mantuvo sus esperanzas hasta el fin de sus días por ver este sueño hecho realidad. A el le digo “Padre lo hemos logrado”.

A mis hermanos OSWALDO STEVENSON Y CRISTIAN STEVENSON que me ayudaron durante todo este proceso, para alcanzar cada una de las metas, a ellos que les tengo gran confianza les dedico este logro.

A mi tío ROQUE STEVENSON por que me dio un gran apoyo y ayuda en los momentos que creí que esta meta no se podía alcanzar.

Y a todos los demás familiares y amigos que de una u otra forma me ayudaron a alcanzar este gran éxito. A todos ellos les digo gracias muchas gracias y espero seguir contando con su apoyo incondicional.

LEONARDO STEVENSON HERNÁNDEZ

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

ACK: (Acknowledgement). Confirmación de recibo de una trama y reconocimiento.

ACL: (Access Control List). Método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

AP: (Access Point). Se encargan de recibir la información de las diferentes TR de los que constituya la red para su centralización o para su encaminamiento.

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

BLUETOOTH: Es una interfaz de radio universal en la banda de frecuencia globalmente disponible en los 2.4GHz que facilita la comunicación de datos y voz tanto en ambientes estacionarios como en ambientes móviles**.**

Buffer: Área temporal de almacenamiento de información que permite recuperarla rápidamente.

CDMA: (Code Division Multiple Access). Esta tecnología asigna códigos únicos a cada usuario, haciendo que las comunicaciones puedan utilizar mejor todo el espectro de frecuencias.

DFS: (Dynamic Frequency Selection). Selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

ESS**:** Es un caso específico del modo infraestructura, representado por un conjunto de BSS asociadas mediante un sistema de distribución.

FHSS: (frecuncy hopping spread spectrum). Espectro ensanchado con salto de frecuencia utilizado en las especificaciones SWAP.

IrDA: (Infrared Data Association). Se constituyó en 1993 para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos.

LANs. Es un sistema que permite conectar las PC y otros dispositivos dentro de la misma red para compartir recursos tales como impresoras, archivos e Internet.

MAC: (Mediwn Acces Control). Es un acrónimo de control de acceso al medio funciona como network que controla y determina quien debe transmitir.

OFDM: (Orthogonal Frequency División Multiplexing). Es un esquema de codificaron que ofrece ventajas sobre el espectro ensanchado en cuanto al canal y tasa de datos.

OSA: (Open System Authentication). Método por el cual cualquier interlocutor es válido para establecer una comunicación con el AP.

PCMCIA: Es una tarjeta de expansión que se utilizan en los computadores principalmente en los portátiles.

PDAs: (Agendas electrónicas personales). Son pequeñas computadoras portátiles que posee una gran gama de funciones como Internet comunicación sincronizada con el PC.

QoS: (Quality of Service). Asegura que los datos importantes viajen en la red antes que los menos importantes. Por ejemplo, las conversaciones de voz tienen la prioridad más alta.

Roaming: Desplazarse fuera de la cobertura de su celda y conectarse a otra manteniendo la continuidad de las aplicaciones que anteriormente ejecutaba

RTCP: Acrónimo de Red Telefónica Pública Conmutada.

SKA: (Shared Key Authentication). Método mediante el cual ambos dispositivos disponen de la misma clave de encriptación.

SSID: (Service Set IDentifier). Cadena de 32 caracteres máximo que identifica a cada red inalámbrica.

SWAP: (Shared Wireless Access Protocol). Ésta tecnología fue derivada de extensiones de tecnologías existentes de Telefonía Inalámbrica-DECT y Wireless LAN para obtener una nueva clase de servicios inalámbricos para el hogar.

TCP/IP: Conjunto de protocolos de comunicaciones que definen cómo se pueden comunicar entre sí ordenadores y otros dispositivos de distinto tipo.

TDMA: (Time Division Multiple Access). Tecnología que divide una frecuencia única en pequeñas fracciones de tiempo.

TKIP: (Temporal Key Integrity Protocol). Codifica las claves mediante un algoritmo de hashing, con verificaciones de integridad adicionales para evitar manipulaciones, Implica modificaciones en el firmware del actual hardware.

TPC: (Transmit Power Control). Este control limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano.

TR: (Tarjetas de red). Recibe y envía la información hacia su destino desde el computador en el que estemos trabajando.

WEP: (Wireless Equivalent Protocol). Asegura la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos.

INTRODUCCIÓN

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

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

Para evitar las restricciones impuestas a la utilización del cable, las conexiones inalámbricas se convierten en la alternativa perfecta por su habilidad intrínseca de sortear obstáculos. Dentro del enorme horizonte de las comunicaciones inalámbricas y la información móvil, las redes inalámbricas van ganando rápidamente adeptos como una tecnología madura y fiable, que permite resolver los inconvenientes derivados de la propia naturaleza del cable como medio físico de enlace en las comunicaciones, muchos de ellos de vital importancia en el entorno de trabajo habitual.

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

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

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

1. WIRELESS PAN

1.1 INTRODUCCIÓN

Las tecnologías inalámbricas y los servicios móviles (Pocket PC, celulares, computadores potables) se han fortalecido en los últimos años y son unos de los campos de mayor crecimiento del sector de las telecomunicaciones. Esto debido fundamentalmente a que la movilidad se ha convertido en un aspecto clave de la sociedad actual. Vivimos en una época de constante cambio donde aparecen nuevas formas de vida, la cuales a su vez generan nuevas necesidades. Las personas desean mantenerse en contacto con sus compañeros, profesores, y tener acceso a la información en todo momento sin importar el lugar donde se encuentren.

El desarrollo de un mundo inalámbrico cambiara fundamentalmente la forma en que los seres humanos consumen, interactúan y controlan sus vidas, abriendo pasos a nuevas sensaciones, experiencias y posibilidades de desarrollo en la universidad. Tareas cotidianas como el pago de una factura o la compra de un libro universitario, serán concebidas de una forma diferente a la que hoy se plantea. La revolución de la información inalámbrica trae consigo un beneficio potencial para las personas y da cabida a la creación de nuevos servicios y productos que antes no hubieran podido imaginarse.

Dentro de las redes inalámbricas existen aspectos que los usuarios desean tener, como son:

Conveniencia: Ya que el beneficiario podrá acceder a su información en cualquier momento y en cualquier lugar. Los dispositivos móviles actuales pueden catalogarse como aquellos que son muy convenientes y aquellos que no lo son de ninguna manera. Es verdad, que cuando una persona viaja, puede almacenar en su dispositivo móvil una gran cantidad de información importante, pero también es cierto que el usuario considerara algunos aspectos del aparato como el peso, el tamaño, la calidad de la pantalla, el teclado dispositivo y las capacidades en cuanto a consumo de energía.

Personalización: Los beneficiarios esperan que se les brinden servicios independientes basados en necesidades particulares del individuo a si como en gustos personales y su posición geográfica. En un ambiente móvil, las limitaciones físicas del dispositivo obligan a construir y automatizar los procesos que se lleven a cabo normalmente en un ambiente fijo.
Los clientes aspirarán en diseñar y construir sus propios procesos, en lugar de tener que aceptar que se los impongan; más aun cuando son ellos quienes

realizan sus propias transacciones desde sus dispositivos personales. La tecnología inalámbrica debe ser escalable e intuitiva

Seguridad: Existe acuerdo general en que la seguridad de la red móvil debe ser superior a la que presenta un ambiente fijo. Existen numerosas formas de asegurar la confiabilidad y fiabilidad de los datos cuando viajan por la red inalámbrica, a si como poderosos mecanismos de encriptación y cifrada de datos, autenticación y autorización de usuarios, han surgido como respuesta a esta necesidad. Sin embargo, aun no puede certificarse que la seguridad sea total.

1.2 CLASIFICACIÓN DE LAS REDES INALÁMBRICAS

Las tecnologías inalámbricas de corto enlace permiten que numerosos dispositivos puedan conectarse de manera espontánea para intercambiar información y dar soporte a una nueva gama de servicios y aplicaciones. La clasificación de las redes PAN son un claro ejemplo del alcance de la tecnología. Estas redes se extienden por completo al dominio del usuario.

No obstante, y pese a la multitud de opciones que se pueden encontrar en el mercado de las telecomunicaciones es indispensable que los proveedores de servicios, los operadores de redes, los desarrolladores de aplicaciones y todos los que hacen parte de la revolución de las telecomunicaciones, comprendan la necesidad de la convergencia para todos los sistemas de telecomunicaciones.

1.2.1 Redes infrarrojas

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

Las ondas infrarrojas se usan para comunicaciones de corto alcance no atraviesan los objetos sólidos lo cual ofrece una ventaja de no interferencia. Además, la seguridad de los sistemas infrarrojos contra espionaje es mejor que la de los sistemas de radio, no es necesario obtener licencia del gobierno para operar un sistema infrarrojo. Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores/emisores en las ventanas de los edificios. Las transmisiones de radio frecuencia tienen una desventaja: que los países están tratando de ponerse de acuerdo en cuanto a las bandas que cada uno puede utilizar, al momento de realizar este trabajo ya se han reunido varios

países para tratar de organizarse en cuanto a que frecuencias pueden utilizar cada uno.
La transmisión Infrarroja no tiene este inconveniente por lo tanto es actualmente una alternativa para las Redes Inalámbricas. El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70´s, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar.
El mismo principio se usa para la comunicación de Redes, se utiliza un transreceptor que envía un haz de Luz Infrarroja, hacia otro que la recibe.
La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un Transreceptor Infrarrojo. Las primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor.

1.2.2 Redes Bluetooth

Es una interfaz de radio universal en la banda de frecuencia globalmente disponible en los 2.4GHz que facilita la comunicación de datos y voz tanto en ambientes estacionarios como en ambientes móviles.

El sistema Bluetooth esta basado en el enlace de radio de corto alcance y de bajo costo, eliminando las necesidades de cables y conexiones entre, ejemplo, celulares, auriculares, computadores potables, impresoras y LANs.

Los dispositivos que incorporan tecnología inalámbrica de Bluetooth tales como laptop o celulares, son especialmente ideales para satisfacer las necesidades inalámbricas de corto alcance que el usuario final necesita.

Su principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo ha ido plagada de diferencias e incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes que ha imposibilitado su rápida adopción.

Características

No necesita conectividad entre los equipos conectados, esto es una gran ventaja si es comparado con otras tecnologías de radio.

Frecuencia de operación: banda de 2.4GHz (2.402GHz y 2.480GHz)

Alcance nominal entre 10 cm. y 10mts.

Baja potencia de emisión (100mW) Sobre todo cuando opera en distancias cortas (hasta 10 mts). Esta potencia es inferior a las de otras tecnologías sin hilos que operan a la misma frecuencia. Para distancias superiores (hasta 100 m) la potencia se incrementa.

Tecnología robusta a las interferencias de otras señales. El modulo radio evita las interferencias de otras señales, buscando y seleccionando una frecuencia adecuada para la transmisión/ recepción. La rapidez en la búsqueda es una de las principales características del sistema bluetooth, Capacidad total de transmisión de 1 Mbit/s.

Esquema de funcionamiento

Un canal asíncrono para datos y otro síncrono para voz, simultáneamente
Tres canales síncronos para voz (64Kbit/s), simultáneamente.
El canal asíncrono de datos pude soportar una comunicación asimétrica (721 Kbits/s y 57.6 Kbit/s en cada sentido) o simétrica (432.6 Kbit/s en ambos sentidos).
Puede establecer conexión punto a punto o punto a multipunto.

Arquitectura y funcionamiento

La unida funcional del sistema bluetooth se denomina piconet. Cada piconet puede tener hasta un máximo de ocho equipos conectados. Cuando el número de equipos es mayor se constituyen varias unidades que se interconectan entre si. Todos los equipos de una unidad se incorporan de igual forma; sin embargo, uno de ellos se configura como reloj que selecciona la frecuencia de operación y sincroniza a todos los aparatos de la piconet, solamente debe haber un equipo piconet maestro y los demás esclavos. En la figura 1 se observa 3 equipos esclavos (la impresora, el celular y la PDA) y un maestro que es la laptop.

Direcciones que se utilizan en el sistema bluetooth:

BD_ADDR: Bluetooth Device Address
AM_ADDR: Active Member Address
PM_ADDR: Parked Member Address
AR_ADDR: Access Request Address

Cada dispositivo presenta una dirección bluetooth. El maestro que es el principal utiliza la dirección asignada AM_ADDR para direccional a todos los dispositivos esclavos dentro del anillo piconet.

FIGURA 1: Sistema piconet de bluetooth

Modelos de uso

Representan escenarios posibles donde aplicaciones Bluetooth pueden tener lugar, en las universidades se podría dar el caso de tener esta tecnología en un laboratorio, o en un lugar especifico que se quiera implementar.

Computadores sin cable

Es el escenario que mejor describe la concepción de Bluetooth como una tecnología para remplazar cables que trasporten datos. Un ejemplo de grandes cantidades de estos cables es un computador de escritorio. En este caso, los periféricos, tales como el ratón, teclado, impresora, dispositivos de juego, parlantes, escáner, etc. (ver figura 2). Pueden tener un alto grado de libertad al no estar conectados por cables, si no por enlace de radio conectados al PC. Este mismo esquema puede emplearse para compartir recursos de hardware, por ejemplo, un periférico puede que no solo sea utilizado por un computador, si no también por una consola de juego, o una impresora puede ser de uso compartido entre dos equipos sin necesidad de usar cable de conexión.

FIGURA 2: Dispositivos bluetooth

Headset

Los Manos Libres o Headset son dispositivos que se usan para permitir a una persona mantener una conversación telefónica sin tener que sostener el teléfono con las manos.

FIGURA 3: Manos Libre Bluetooth

Puente a Internet

Existen dos métodos para el uso de Bluetooth como un puente inalámbrico para establecer comunicaciones con redes LAN o Internet:

Marcación telefónica: esta forma de acceso a Internet es muy similar a la que se emplea hoy en día: un arreglo convencional implica la presencia de un computador que se use en línea telefónica para conectar a un proveedor de servicio de Internet a través de un modem. Lo que Bluetooth suprime a este escenario es la presencia de cables (entre el modem y la línea telefónica). Mediante el uso de un computador y un teléfono (sea este celular u fijo) equipados con Bluetooth que soporten un perfil para marcar a redes, la conexión a Internet puede realizarse de forma inalámbrica.

Acceso directo ala red: el acceso a Internet por medio de LAN se realiza a través de un gateway sin que halla necesidad de efectuar una marcación telefónica. El acceso directo a la red por medio de bluetooth es posible utilizando dispositivos punto a punto. Se puede decir entonces que Bluetooth proporciona un conector inalámbrico para la conexión a redes.

1.2.3 HOMERF

Introducción

El mundo de los denominados datos inalámbricos incluye enlaces fijos de microondas, redes LAN inalámbricas, datos sobre redes celulares, redes WAN inalámbricas, enlaces mediante satélites, rayos infrarrojos difusos y por línea de vista, comunicaciones basadas en láser y mucho más. Se analizará la tecnología la tecnología HomeRF, la cual opera en la banda ISM de los 2,4GHz y está basada en el protocolo inalámbrico de Acceso Compartido (Shared Wireless Access Protocol, SWAP), tecnología que encamina sus pasos hacia la conectividad sin cables dentro del hogar. Los principales fabricantes de estos sistemas se agrupan en torno al consorcio que lleva su mismo nombre: HomeRF Working Group.

La especificación SWAP define una nueva interfaz como inalámbrica que está diseñada para poder soportar tanto el tráfico de voz como los servicios de datos en redes LAN dentro los entornos domésticos e ínter operar con las redes publicas de telefonía e Internet. Esta nueva normativa ha sido definida para asegurar la interoperatividad de una numerosa cantidad de productos con capacidades de comunicación inalámbricas que se desarrollan para computadoras del mercado doméstico, permitiendo que los computadores, periféricos, teléfonos y electrodomésticos puedan comunicarse con otros dispositivos de similar naturaleza sin la obligada presencia de los molestos cables de interconexión.

Asimismo, la arquitectura del protocolo se asemeja bastante a las especificaciones que tiene IEEE 802.11 en su capa física para las redes inalámbricas, adicionalmente extiende la capa MAC (Mediwn Acces Control) con la adición de un subconjunto de estándares DECT para proporcionar los servicios de voz. Como resultado, la capa MAC puede soportar indistintamente servicios orientados a datos, tales como TCP/IP, y los que se orientan a voz como DECT/GAP (tecnología que permite la implementación de servicios de voz por medio de terminales inalámbricos).

HomeRF WORKING GROUP

Fundado en marzo de 1998, el Grupo DE TRABAJO HomeRF (HomeRF Working Group), tiene como misión conseguir la interoperatividad entre el mayor número de dispositivos diferentes que estén ubicados en cualquier punto del hogar. Para ello establecen un estándar abierto y sin licencia basado en comunicación digital mediante Radio Frecuencia. El resultado ha sido el desarrollo de SWAP (Shared Wireless Access Protocol).

Home Working Group, está compuesto por muchas empresas de las que se destacan: Compaq, Intel, Motorola, Semiconductor Nacional, Proxim y Siemens. Estas seis empresas trabajaran para establecer el despliegue masivo de una red de datos con acceso inalámbrico ínter operable para dispositivos de voz, datos y multimedia en el ambiente consumidor. Cada uno de los seis promotores representa una ficha clave en el sector de la industria en el desarrollo final de SWAP 2.0, el cual esta siendo diseñado para soportar velocidades de 10Mbps Ethernet, manteniendo al mismo tiempo costos, rangos de interferencia, etc.

Además, pueden destacar otras empresas que hace parte del HomeRF Working Group como: Ericsson Enterprise Networks, Hewlett-Packard, IBM, Microsoft, Philips Consumer Comunications, Cisco Systems, Harris Semiconductor, Intellon, National Semiconductor, Nortel, Rockwell Semiconductor y Samsung. El amplio rango de industrias representadas, asegura que la especificación es razonablemente completa en todos los sectores.

Visión General de HomeRF

Dos factores han sido muy importantes para el establecimiento de una red de datos dentro del hogar, una oportunidad verdadera de tener éxito.

El crecimiento explosivo de Internet es un factor primario. Internet ofrece una oportunidad para revolucionar el intercambio de información y entretenimiento dentro del hogar.

La presencia en el mercado de computadores personales más baratos es también un factor crucial en el uso de Internet y el PC en el hogar. La existencia de PC's por debajo de $1000 US permite a todos los grupos familiares de medianos ingresos tener un PC si así lo quieren.

Especificación SWAP

El sistema del Protocolo Inalámbrico de Acceso Compartido HomeRF está diseñado para llevar tráfico de datos y de voz y para ínter operar con la Red Telefónica Pública Conmutada (RTCP) e Internet. Opera en la banda de los 2400 MHz y utiliza espectro ensanchado con salto de frecuencia (frecuncy hopping spread spectrum – FHSS).

La tecnología SWAP fue derivada de extensiones de tecnologías existentes de Telefonía Inalámbrica-DECT y Wireless LAN para obtener una nueva clase de servicios inalámbricos para el hogar.
SWAP soporta TDMA para ofrecer servicios interactivos como voz y otros servicios de tiempo crítico y CSMA/CA para la entrega de paquetes de datos a alta velocidad.

PARAMETROS	VALOR
Saltos de frecuencias de la red	50 saltos/seg
Rango de frecuencias	2400MHz banda ISM
Potencia de transmisión Tasa de datos	100Mw 1 Mbps usando modulación 2FSK 2 Mbps usando modulación 4FSK
Rango de cobertura	Una casa típica (hasta 50 metros)
Estaciones soportadas	Hasta 127 dispositivos por red
Estaciones soportadas	Hasta 6 conversaciones full duplex
Seguridad en datos	Algoritmo de encripción Blowfish (sobre 1 trillón de códigos)
Compresión de datos	Algoritmo LZRW3-A
ID de red de 48 bits	Permite operación concurrente de múltiples redes

TABLA 1: Principales parámetros de HomeRF

Control de Acceso al Medio (MAC) para HOMErF 1.0

El MAC de SWAP ha sido optimizado para el entorno de un hogar y está diseñado para llevar tráfico de voz y de datos e ínter operar con la RTCP utilizando un subconjunto de DECT. El MAC está diseñado para trabajar con saltos de frecuencia y también incluye un servicio TDMA para soportar la entrega de datos síncronos así como CSMA/CA, un servicio derivado de los estándares de Wireless LAN tal como IEEE 802.11 y Open Air para soportar la entrega de datos asíncronos. El MAC de SWAP provee las siguientes características:

Buen soporte para voz y datos usando mecanismos de acceso TDMA y CSMA/CA.
Soporte para cuatro conexiones de voz de alta calidad con ADPCM de 32Kbps.
Transmisión de datos de 1.6Mbps.
Seguridad de datos con niveles ninguno/básico/robusto de encriptación.
Administración de energía para dispositivos síncronos y asíncronos.
Identificador de red de 24 bits.

1.2.4 Tecnología HOMERF 2.0

HomeRf 20 tiene el respaldo de grandes de la industria como Intel y Proxim. Además, el HomeRf Working Group afirma que la versión 2 ofrece numerosas ventajas sobre 802.11b.

HomeRf 2.0 incluye soporte hasta 4 handsets telefónicos inalámbricos que funcionan igual que la línea telefónica estándar con identificador de llamadas y otras características ya comunes.

Velocidad mejorada

HomeRF 1.0 corría a 1.6Mbps, una velocidad aceptable para compartir Internet pero no suficiente para transmisión de archivos grandes como mp3 y videos. HomeRF 2.0 incrementa el ancho de banda a 10Mbps, la misma velocidad del estándar Ethernet.

Seguridad

El modelo de seguridad de HomeRf 2.0 es relativamente transparente al usuario final y muy efectivo. HomeRF 2.0 usa la tecnología de saltos de frecuencia y el concepto “network password” o contraseña de red que es necesaria para vincularse a la red, sin el password, los periféricos son incapaces de comunicarse con la red. Ahora HomeRF 2.0 incluye soporte para encripción de 128 bits de tal forma que todo el tráfico a través de la red es ilegible por dispositivos terceros.

Resistencia a la interferencia

802.11b o Wireless Ethernet está expuesto a interferencia en la banda de los 2.4GHz usada por algunos teléfonos inalámbricos. HomeRF 2.0 también usa esa banda, pero hace un seguimiento en las diferentes clases de interferencia presentes alrededor del área de trabajo. Eso se hace identificando en que canal de datos este presente la interferencia para que el proceso de salto de frecuencia no use ese canal. HomeRF 2.0 no interfiere con la tecnología Bluetooth.

Soporte para comunicaciones de voz

El soporte para comunicación de voz en HomeRF 2.0 es el estándar europeo DECT. Usando esta tecnología, HomeRF 2.0 soporta hasta 8 conversaciones simultáneas y hasta 8 teléfonos

QoS – Calidad de servicio

El manejo del QoS garantiza el ancho de banda y da prioridad a los paquetes en la red. Cuando la red es utilizada para soportar múltiples servicios, como conversaciones de voz, transferencia de archivos y acceso a Internet, QoS asegura que los datos importantes viajen en la red antes que los menos importantes. Por ejemplo, las conversaciones de voz tienen la prioridad más alta para mantener la calidad en el audio.

Bajos Requerimientos de potencia

HomeRF 2.0 fue diseñado no solo para computadores, su chipset es muy pequeño y usa muy poca potencia, haciéndolo apropiado para incorporarlo en dispositivos como Web Pads, teléfonos inalámbricos para Internet, PDA's.
Recepción: 3.3v, 120mA
Transmisión: 250mA
Standby: 3mA

Información adicional

Compatibilidad con HomeRF 1.0.
Soporte incluido para roaming (saltos entre múltiples puntos de acceso).

2. ESTÁNDARES IEEE PARA REDES INALÁMBRICAS

2.1 HISTORIA

La historia de las WLAN es bastante reciente, de poco más de una década. En 1989, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN, pero no es hasta 1994 cuando aparece el primer borrador, y habría que esperar hasta el año 1999 para dar por finalizada la norma.

En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems). En 1993 también se constituye la IrDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de informática móvil (mobile computing) y de

servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios ínter operativos. Por otra parte, WLANA (Wireless LAN Association) es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original que llego a velocidades de 2 Mbps ; 802.11a (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; 802.11b hasta 11 Mbps, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, 802.11g, compatible con él, pero que proporciona aún mayores velocidades de hasta 54 Mbs, 802.11e es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN, 802.11i que es un estándar de seguridad entre otros

2.2 IEEE 802.11A

El instituto de ingenieros eléctricos y electrónicos IEEE desarrollo esta especificación que representa nuevas generaciones en las redes inalámbricas de área local. Esta diseñada para trabajar en la banda de 5GHz llamada banda nacional de infraestructura de información (U-NII). Utiliza 300MHz de esta banda dado por la FCC, esta dividida en tres bandas de 100MHz, dos de las cuales son contiguas; para cada una de estas bandas se restringe la potencia RF máxima de transmisión de acuerdo a la tabla 2.

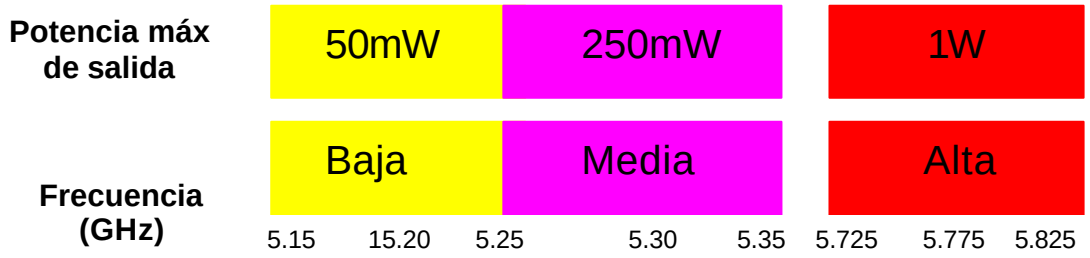

TABLA 2: Distribución de las bandas de frecuencia

En esta distribución, de bandas de frecuencia se ha establecido que las aplicaciones variaran desde las aplicaciones entre edificios (bulding to bulding) para la banda alta hasta las aplicaciones en interiores (in- building). Los productos que utilizan la banda bajas siempre deben usar antenas integradas según la especificación.

El rango de frecuencia actualmente utilizado para la mayoría de transmisiones sin licencia, incluyendo 802.11b, es la banda ISM de 2.4GHz. Esta banda utilizada por un gran número de tecnologías ofrece solamente 83MHz para todo el tráfico inalámbrico, incluyendo teléfonos inalámbricos, transmisiones de edificio a edificio, y hornos microondas. En comparación, a los 300MHz ofrecidos por la banda U-NII representa un aumento de cuatro veces en espectro, además por el momento existen muy pocas tecnologías que utilizan esta banda.
Para Colombia rigen rangos de frecuencia de 5.15 - 5.35 GHz; 5.425 – 5.675 GHz; 5.725 – 5.875 GHz, para una cobertura de hasta 150 m

El esquema de modulación que se presenta en 802.11a es OFDM (Orthogonal Frequency División Multiplexing) con el fin de optimizar la disponibilidad de canales respecto a la tecnología de espectro ensanchado que utiliza 802.11b.

La Multiplexacion por División Orthogonal de Frecuencia (OFDM), es un esquema de codificaron que ofrece ventajas sobre el espectro ensanchado en cuanto al canal y tasa de datos. La disponibilidad del canal es significativa porque hay mas canales independientes disponibles, así la red se vuelve mas escalable.

Para lograr las altas tasa de datos se combinan muchas su-portadoras de baja velocidad para crear un canal de alta velocidad. 802.11a utiliza OFDM para definir un total de 8 canales sin traslapamiento de 20Mhz a través de las dos bandas más bajas; cada uno de estos canales se divide en 52 sub-portadoras, de aprox. 300 KHz de ancho. Comparando, 802.11b utiliza 3 canales sin traslapamiento.
Las sub-portadoras se transmiten en paralelo, lo cual significa que se envían y se reciben simultáneamente. El dispositivo receptor procesa estas señales individuales, donde cada una representa una fracción de los datos totales que, juntos, crean la señal real. Con estas múltiples sub-portadoras abarcando cada canal, una enorme cantidad de información puede ser enviada de una vez.

Velocidad

Los dispositivos que trabajen bajo este estándar soportaran velocidades de 6, 12, y 24 Mbps; opcionalmente existen velocidades de 9, 18, 36 y 48Mbps; estas velocidades se soportan gracias a las técnicas de modulación y niveles diferentes de corrección de errores (se utiliza el esquema FEC o Forward Error Correction). Se puede lograr una velocidad máxima de hasta 54Mbps utilizando el mecanismo de modulación 64QAM para poder montar la mayor cantidad de información posible permitida por el estándar en cada subportadora.

De acuerdo a la distancia a la que se encuentre un dispositivo del punto de acceso, la velocidad efectiva a la que este puede transmitir información con calidad, se decrementa. En la siguiente figura se puede observar una comparación de este efecto en 802.11a y 802.11b (cuya velocidad se ve mas disminuida con la distancia entre las estaciones)

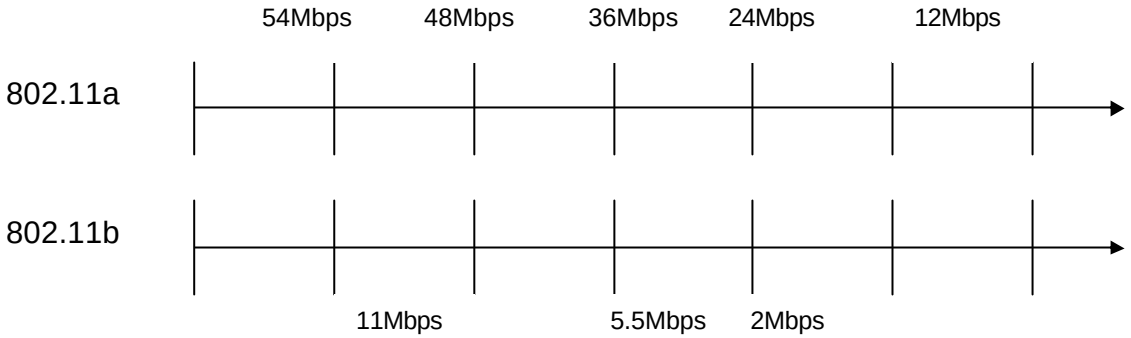

FIGURA 4: Comparación de alcance de 802.11a y 802.11b

Seguridad

Dado que las señales inalámbricas viajan a través de un medio compartido, este medio puede ser accedido y se podrían interceptar las comunicaciones que se estén llevando a cabo; se deben utilizar mecanismo de encriptación y de autenticaron cada ves que se implemente un sistema inalámbrico de transmisión de datos. (Ver seguridad en WI-FI)

Manejo de la interferencia

La especificación predice el efecto de interferencia por multitrayecto, cuando una señal abandona la antena, es susceptible de tomar muchos caminos, incluso reflejarse, ante de llegar al receptor; el resultado de esta condición es la posible anulación de la señales en el trayecto; para ello, el procesador de banda base debe discriminar las señales divergentes. Pero, cabe la posibilidad de que una señal reflejada se retrase lo suficiente como para interferir con la siguiente transmisión; por ello la modulación OFDM especifica una velocidad de símbolos baja con el fin de reducir la probabilidad de coalición de estas señale con nuevas transmisiones.

Dado que la especificación de 802.11a y 802.11b son diferentes en su nivel físico, (puesto que trabajan en frecuencia de 5GHz y 2.4GHz respectivamente) son incompatibles en este sentido y no se interfieren sus señales.

Otra característica que reduce la interferencia es que utiliza los mensajes de confirmación- ACK a nivel de la capa AMC (Media Access Control) lo cual la hace más robusta frente a las fallas y aumenta al máximo el uso del ancho de banda del canal de radio. También realiza control de secuencia de mensaje, identificando a cada uno con un número de secuencia determinado que servirá después para llevar un control de toda la comunicación.

Potencia

Existe un mecanismo empleado para reducir el consumo de potencia (generalmente en dispositivos con batería) y que consiste en entrar en estados de bajo consumo o de consumo nulo en caso de haber transcurrido cierto tiempo de inactividad. Esto puede ocasionar problemas, ya que puede perderse información valiosa durante estos periodos de adormecimientos; para solucionar esto, los puntos de acceso tienen buffer que les permiten almacenar colas de mensajes que vaya n hacia estaciones que estén en periodos de bajo consumo. Las estaciones periódicamente tendrán que despertar y recibir dichos mensajes, de lo contrario, los puntos de acceso podrán descartarlos luego de cierto tiempo.

2.3 IEEE 802.11

Como una autoridad reconocida globalmente, el comité 802 de la IEEE ha establecido los estándares que han guiado la industria de las LAN desde hace dos décadas, incluyendo 802.3 Ethernet, 802.5 Token Ring y 802.3z 100BASE-T Fast Ethernet. En 1997, luego de siete años de trabajo, la IEEE publico la norma 802.11, el primer estándar sancionado internacionalmente para las redes de área local inalámbricas.
Como todos los estándares IEEE, el 802.11 se enfoca en los niveles inferiores del modelo ISO, el nivel físico y el nivel de enlace de datos. Cualquier aplicación de LAN, sistemas operativos o protocolos, incluyendo TCP/IP podrá trabajar sobre una red WLAN que cumple con 802.11 de la misma manera que lo hace sobre la tradicional Ethernet.

Modos operacionales de 802.11

802.11 define dos piezas de equipo, una estación inalámbrica (STA - station), que normalmente es un PC equipado con una tarjeta de red inalámbrica (W-NIC) y un punto de acceso (AP- Access Point), que actúa como un puente entre las redes cableadas y la inalámbrica. Un AP normalmente costa de un radio, una interfaz de red cableada y un firmware que soporta el estándar (802.1d). El AP soporta el acceso de múltiples STAs A la red cableada. Las STAs pueden tener tarjetas 802.11 PCMCIA, PCI o ISA o pueden ser dispositivos con capacidades 802.11 embebidas.

Sus principales ventajas es su velocidad de 2Mbps, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

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

2.4 IEEE 802.11b

En septiembre de 1999 la misma IEEE ratifico la mejora 802.11b al primer estándar, lo que agrego dos velocidades mas altas (5.5 y 11 Mbps) a estándar original 802.11 y otras características como el cambio de taza de transferencia dinámico DRS (Dynamic Rate Shifting), la cual permite a los adaptadores de red reducir las velocidades para compensar los posibles problemas de recepción debido exclusivamente a distancias y materiales que se deseen atravesar

Con las WLANs 802.11b, los usuarios móviles pueden alcanzar niveles comparables a Ethernet en cuanto a desempeño, velocidad y disponibilidad. Esta tecnología basada en estándares permite a los administradores construir redes que sin problemas combinan más de una tocología LAN para atender de mejor manera las necesidades del negocio y los usuarios. Información completa en el capitulo 4

2.5 IEEE 802.11g

El estándar IEEE 802.11g alcanza velocidades más altas hasta de 54Mbps y es compatible con los equipos 802.11b ya existentes. El 802.11g opera en la misma banda de frecuencia de 2,4GHz, sin necesidad de licencia y con los mismos tipos de modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes.
Esta compatibilidad con versiones anteriores protege la inversión de los clientes en varios aspectos. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps. Para lograr velocidades más altas, de hasta 54 Mbps, tanto el punto de acceso como la tarjeta de red deben ser compatibles con el estándar 802.11g. El estándar también especifica tipos de modulación opcionales como el OFDM/CCK (Orthogonal Frequency División Multiplexing). El cual es un esquema de codificaron que ofrece ventajas sobre el espectro ensanchado en cuanto al canal y tasa de datos. Diseñados para mejorar la eficiencia en una instalación íntegramente 802.11g. En instalaciones grandes, la ventaja de tener aproximadamente los mismos alcances de transmisión efectivos es que la estructura WLAN 802.11b ya existente se puede mejorar fácilmente para lograr velocidades más altas sin necesidad de instalar puntos de acceso adicionales en muchos lugares nuevos a la hora de cubrir una zona determinada.
En comparación con el estándar IEEE 802.11a, el 802.11g tiene un ancho de banda utilizable más bajo, lo que redunda en un menor número de usuarios WLAN

de alta velocidad. Aunque las modulaciones OFDM permiten una velocidad más alta, el ancho de banda disponible total en la banda de frecuencia de 2,4GHz no varía.

2.6 IEEE 802.11e

El objetivo de dicho estándar es la mejora del nivel MAC del 802.11 para el aumento y la gestión de la QoS (Quality of Service), proporcionar una serie de servicios y mejorar el mecanismo de seguridad y autentificación. El objeto es permitir una gestión más eficaz de la banda en presencia de aplicaciones multimedia (voz, imagen y sonido).

El programador centralizado usado en la QoS Baseline garantiza que no habrá colisiones y mejora además la capacidad para entregar contenidos sensibles a los retardos mediante el control de la latencia, el jitter y el ancho de banda. Para conseguir la fiabilidad del sistema, el acceso a canal saca partido de los mecanismos y protocolos de alto nivel que gestionan el ancho de banda de la subred.

2.7 IEEE 802.11f

Presenta una interoperabilidad de Puntos de Acceso (AP) dentro de una red WLAN multiproveedor. El estándar define el registro e Puntos de Acceso (AP) dentro de una red y el intercambio de información entre dichos Puntos de Acceso cuando un usuario se traslada desde un punto de acceso a otro.

2.8 IEEE 802.11h

Con el objeto de que los productos 802.11a cumplan con los requisitos europeos, era necesario mejorar el estado MAC del 802.11 y la capa física PHY del 802.11a en la banda de los 5GHz. La intervención pretendía añadir dos funcionalidades DFS (Dynamic Frequency Selection) y TPC (Transmit Power Control).
El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

2.9 IEEE 802.11i

Este estándar surgió a raíz de las vulnerabilidades del 802.11b y es aplicable a redes 802.11a (54Mbps), 802.11b (11Mbps) y 802.11g (22Mbps).
La vulnerabilidad de las transmisiones inalámbricas ha supuesto el desarrollo del nivel MAC para mejorar los mecanismos de autentificación y seguridad. La materia es muy amplia y en su definición los factores afectados tienen posturas muy diferentes.

TKIP (Temporal Key Integrity Protocol), codifica las claves mediante un algoritmo de "hashing", con verificaciones de integridad adicionales para evitar manipulaciones, Implica modificaciones en el firmware del actual hardware.

Norma	Banda de frecuencia	Modulación	Alcance	Velocidad máxima	Nº máx. canales sin solap.
802.11 b	2.4GHz	DSSS	100 m	11 Mbps	3
802.11 a	5GHz	OFDM	50 m	54 Mbps	12
802.11 g	2.4GHz	OFDM	100 m	54 Mbps	3
802.11 d 802.11 e	Aspectos reglamentarios en países sin normativa vigente sobre 802.11 Define niveles de QoS				
802.11 f	IAPP (Inter Access Point Protocol)				
802.11 h	Mejora de 11 a en potencia y selección de canal de radio				
802.11i	Mecanismos de seguridad – AES (Advanced Encryption Standard)				
802.11 j	Resuelve la adición del canal 4.9GHz al de 5GHz para 11 a en Japón				

TABLA 3: Cuadros y gráficos representativos al estándar IEEE

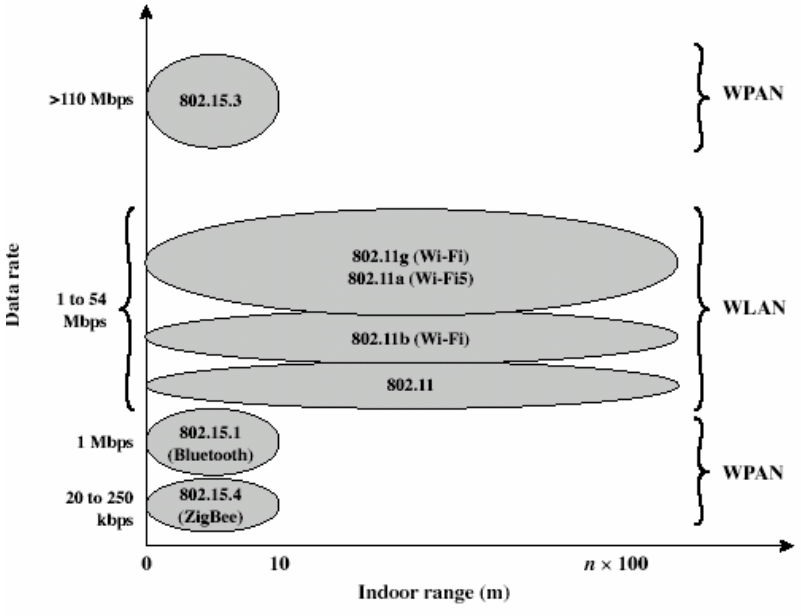

FIGURA 5: Gráficos representativos al estándar IEEE

3. DISPOSITIVOS WIRELESS

3.1 TARJETAS DE RED (TR) Y ADAPTADORES

Serán los que tengamos integrados en nuestro computador, o bien conectados mediante un conector PCMCIA ó un adaptador USB si estamos en un portátil o en un Slot PCI si estamos en un computador de mesa. Substituyen a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el computador en el que estemos trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.
Algunos ejemplos de las mismas:

Tarjeta PC Inalámbrica de 54Mbps 802.11g

Una tarjeta PC inalámbrica de 54Mbps Cumple con el estándar IEEE 802.11g, haciéndola compatible en retroceso con las redes 802.11b para tener una compatibilidad asegurada mientras se navega entre redes. El acceso protegido Wi-Fi avanzado (WPA) y hasta 256bit de encriptación WEP son respaldados para proporcionar acceso seguro para su banco de datos, Cobertura de distancia en el interior de 35~100 metros, exterior de 100~300 metros (dependiendo del fabricante). En la figura 6 se observan varias tarjetas inalámbricas que están conectadas ya sea a un equipo de escritorio o a un laptop, estas reciben una señal proveniente de un Switche, para tener acceso a Internet.

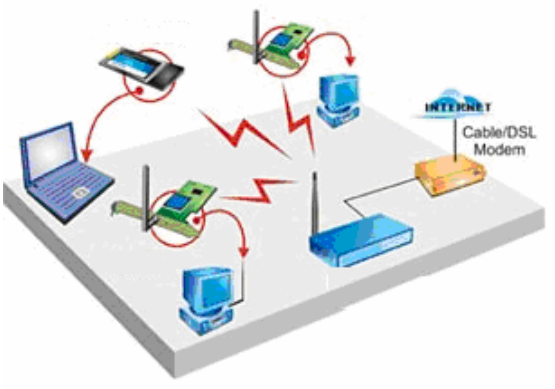

FIGURA 6: Tarjetas PC Inalámbricas

Adaptador Bluetooth USB

El Adaptador USB Bluetooth permite hacer conexiones inalámbricas de corto alcance entre su computadora y dispositivos permitidos Bluetooth tales como teléfonos celulares, PDAs impresoras y computadoras. Es compacto y portátil, eliminando así la necesidad de usar cables y conexiones físicas entre dispositivos electrónicos. La transmisión del Adaptador USB Bluetooth asegura protección en contra de interferencia y transferencia de datos segura, Sincroniza automáticamente dispositivos en la red de área personal "Personal Area Network" (PAN) para mantener datos constantes, rango de conectividad de hasta 10 metros. Estas características varían con el fabricante. (Ver figura 7)

FIGURA 7: Adaptador bluetooth

3.2 PUNTOS DE ACCESO (PA)

Se encargan de recibir la información de las diferentes TR (Tarjetas de Red) de los que constituya la red para su centralización o para su encaminamiento, en un nodo especial de la red inalámbrica. Complementan a los Hubs, Switches o Routers, disponen comúnmente de una internas Ethernet que les permite estar interconectados a una red cableada LAN, cuando exista mas de un punto en la zona las frecuencias de funcionamiento no deben interferir fuertemente entre si. Sin embargo, los últimos dispositivos del mercado no tienen este problema. La velocidad de transmisión / recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

Punto de acceso para 802.11g de 54Mbps

La Base Transmisora Inalámbrica de 54Mbps interconecta las redes cableadas e inalámbricas. Conforme con la norma IEEE 802.11g y 802.11b, estos dispositivos provee una operación con espectro de difusión de secuencia directa "Direct Sequence Spread Spectrum (DSSS) para bridging transparente y capacidad de roaming para los nodos inalámbricos. Presentan funciones bridging AP-to-AP, permitiendo a los usuarios conectar dos o más puntos de acceso a la vez de forma inalámbrica. Con esta base transmisora y los adaptadores de redes inalámbricos, los usuarios podrán conectarse a la LAN Ethernet/Fast Ethernet en casa o en la oficina para acceder a recursos de redes como discos duros, drives CD-

ROM/DVD, impresoras de red, y conexión a Internet. Los dispositivos de IEEE 802.11b abarcan distancias de 35 a 60 metros en el interior, 100 a 300 metros en el exterior, Los dispositivos de IEEE 802.11g abarcan distancias de 20 metros en el interior, 50 metros en el exterior. En la figura 8 se observa un punto de acceso con varios terminales inalámbricos y una conexión de cable DSL con acceso a Internet.

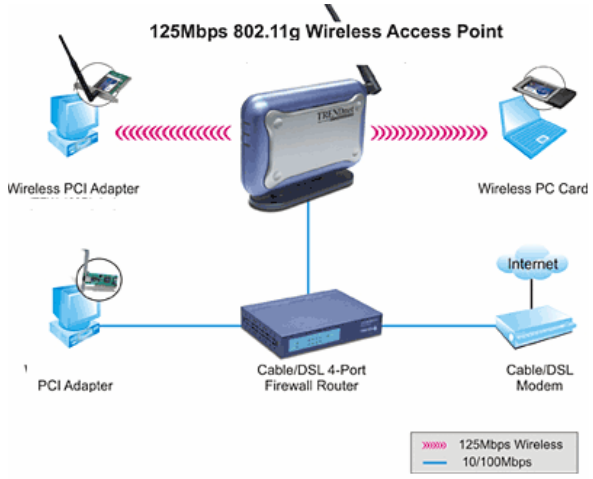

FIGURA 8: Configuración de un punto de acceso

3.3 ROUTERS

Estos dispositivos no tienen un funcionamiento total de routers inalámbrico puesto que en su gran mayoría son usados como interfases entre la LAN y la red inalámbrica, por esta razón poseen un puerto el cual le da acceso a la red cableada existente.

Trabajan en la capa 3 y 4 del modelo OSI, poseen una estructura interna bastante compleja lo que facilita para realizar funciones especificas de encriptación WEP de 128bit para transferencia inalámbrica de datos. También, limita el acceso a contenidos indeseables controlando el camino a la Web vía URL u Hora/Fecha. Su Instalación es fácil como una herramienta de configuración, algunos dispositivos también presentan características como Soporte en Protección Firewall y el Soporte al Servidor Virtual de hasta de 20 canales.

Se utilizan en enlaces punto a punto, o en topologías como maya y estrella.

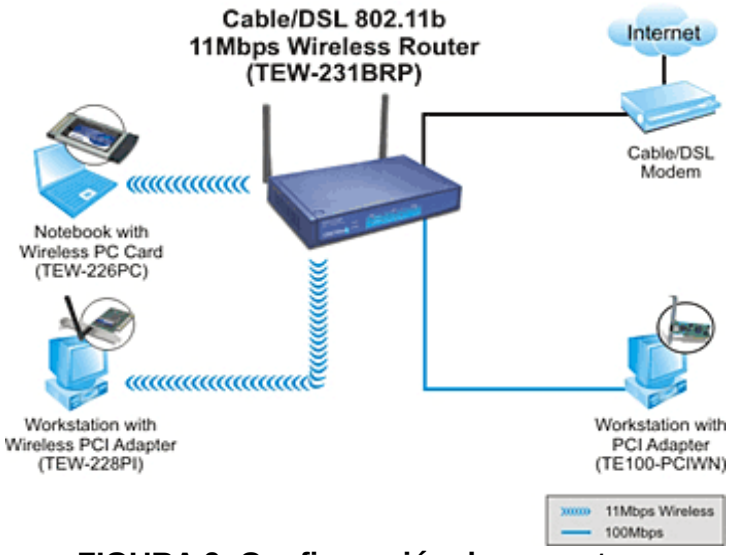

FIGURA 9: Configuración de un routers

3.4 ANTENAS Y PUENTES

Existen dos clases de antenas principales que son:
Las antenas Direccionales envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual presenta un alcance mayor, sin embargo fuera de la zona de cobertura, no se puede establecer comunicación entre los interlocutores.

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

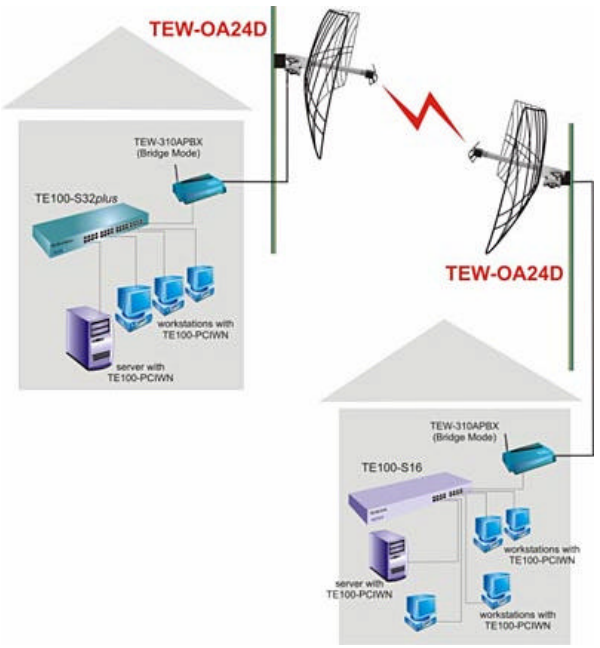

FIGURA10: Antenas punto a punto

4. ARQUITECTURA INTERNA DE LAS REDES WI-FI

4.1 INTRODUCCIÓN

El elemento fundamental de la arquitectura de las redes 802.11 es la celda la cual se puede definir como el área geográfica en la cual una serie de dispositivos se interconectan entre si por un medio aéreo. En general estas celdas están compuestas por las estaciones y un único punto de acceso (AP). Las estaciones son adaptadores que permiten la conversión de información generalmente encapsulada bajo el protocolo Ethernet existente en terminales o equipos clientes, y su envío y recepción dentro de la celda. El punto de acceso es el elemento que tiene la capacidad de gestionar todo el tráfico de las estaciones y que pueden comunicarse con otras celdas o redes. Es a todos los efectos un bridge que comunica a nivel 2 los equipos tanto de su celda de cobertura como a otras redes a las cuales estuviese conectado. A esta configuración se le denomina grupo de servicios rápidos (Basic Service Set, BSS). El BSS es por tanto una entidad independiente que puede tener su vinculación con otras BSS a través del punto de acceso mediante un sistema de distribución (Distribution System, DS). El DS puede ser integrado (comunica el BSS con una red externa), o también inalámbrico, en cuyo caso se denomina WDS (Wireless Distribution System).

4.2 MODO DE OPERACIÓN DE LAS REDES WI-FI

El modo de operación de las redes WI-FI es la arquitectura de las redes, en forma de celda, la cual se puede definir como el área geográfica en la cual una serie de dispositivos se interconectan entre sí por un medio aéreo. En general esta celda estará compuesta por estaciones y un único punto de acceso. Las estaciones son adaptadores que permiten la conversión de información generalmente encapsulada bajo el protocolo ethernet existente en terminales o equipos, y un envió y recepción dentro de la celda. El punto de acceso es el elemento que tiene la capacidad de gestionar todo el tráfico de las estaciones y que puede comunicarse con otras celdas o redes.

4.2.1 BSS independiente (IBSS)

Es una celda inalámbrica en el cual hay un conjunto de dos o mas estaciones que se comunican entre si a través de un punto de acceso, por esta razón posee un rango de cobertura bastante elevado gracias al AP, el numero de equipos que forman parte de ella dependerá directamente de las prestaciones del AP, no presenta sistema de distribución y por tanto, no tiene conexión con otras redes

FIGURA 11: Modo IBSS de redes WI-FI

4.2.2 Modo Ad –hoc

Es una variante del IBSS en el cual no hay punto de acceso. Las funciones de coordinación son asumidas de forma aleatoria por una de las estaciones presentes. El tráfico de información se lleva a cabo directamente entre los dos equipos implicados, sin tener que recurrir a una jerarquía superior centralizadora obteniéndose un aprovechamiento máximo del canal de comunicaciones. La cobertura se determina por la distancia máxima entre dos equipos, la cual suele ser apreciablemente inferior a los modos en los que hay un punto de acceso. Es un modo de empleo infrecuente por las connotaciones de aislamiento que
Con lleva, aunque puede ser muy útil cuando el tráfico existente se reparte entre todos los equipos presentes.

FIGURA 12: Modo Ad-hoc

4.2.3 Modo infraestructura

el punto de acceso realiza las funciones de coordinación, todo el trafico tiene que atravesarlo, por lo que hay una clara perdida de eficiencia cuando dos estaciones dentro de un mismo BSS desean comunicar entre si (los paquetes de información son enviados una vez al punto de acceso y otra vez al destino). Es una arquitectura apropiada cuando la mayor parte del tráfico se origina o finaliza en las redes exteriores a las cuales esta conectado el AP. La cobertura alcanza una distancia cercana al doble de la distancia máxima entre el punto de acceso y estación. Es el modo que se emplea habitualmente para conectar una red inalámbrica con redes de acceso a Internet.

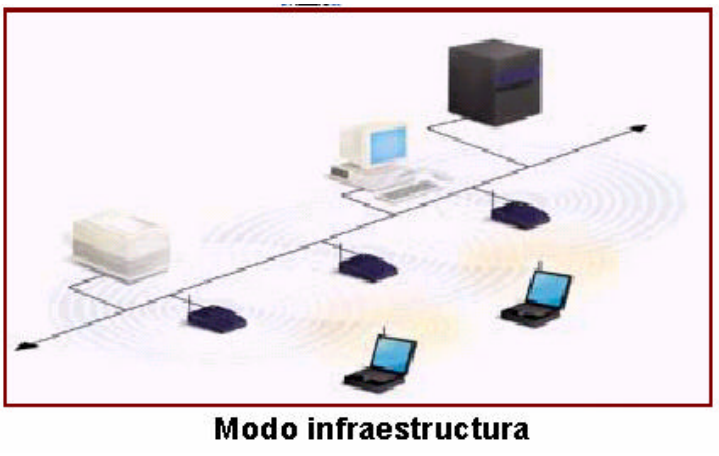

FIGURA 13: Modo infraestructura

4.2.4 BSS Extendido (ESS)

Es un caso específico del modo infraestructura, representado por un conjunto de BSS asociadas mediante un sistema de distribución. Esto permite una serie de prestaciones avanzadas opcionalmente como el roaming entre celdas.

Para poder identificar de manera inequívoca a las celdas inalámbricas se les asigna un nombre de red consistente en una cadena con longitud máxima de 32 caracteres denominado Service Set IDentifier, SSID. Para poder agregarse a una determinada celda es requisito indispensable que el equipo tenga en su configuración interna el mismo SSID. Si se desea que la estación se conecte a cualquier celda inalámbrica presente, se deberá poner como parámetro ANY. Inmediatamente el equipo analizara todas las celdas que estén presentes y se conectara a una de ellas adoptando su SSID, generalmente con el criterio de la que mayor nivel de señal posea

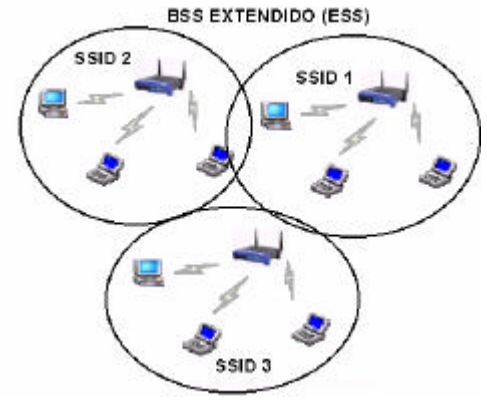

FIGURA 14: BSS extendido

4.3 SERVICIOS

4.3.1 Servicios de la estación

Con el fin de establecer los mecanismos internos que rigen los procesos mas básicos en las redes WI-FI dentro de las recomendaciones IEEE 802.11 se han definidos cuatro servicios elementales que afectan a la operativa de las estaciones que se conectan a un punto de acceso:

Autentificación
Todo equipo que desee conectar a un BSS deberá identificarse, comunicándole la resolución. Si le deniega el permiso, la estación no podrá luego proceder a la asociación a la celda. Una estación puede solicitar la autentificación a varias BSS.

En el caso que se desee conceder el acceso libre, el punto de acceso responderá siempre positivamente a cualquier solicitud

Des-autentificación
Es el proceso inverso por el que una estación solicita darse de baja en la lista de equipos permitidos

Envío de datos (data delivery)
Por medio de este servicio los equipos gestionan el flujo de datos desde y hacia la celda

Privacidad
Existen diversos mecanismos de seguridad de la información que serán tratados en el ítem de seguridad

4.3.2 Servicios de distribución

Gestionan la relación de un equipo con una determinada celda y hacia donde debe ser enviada la información

Asociación
De entre los puntos de acceso a los que está autenticada la estación deberá elegir uno al que conectarse. Esto se realiza mediante un proceso de asociación por medio del cual la dirección MAC del equipo queda registrada en las tablas del AP.

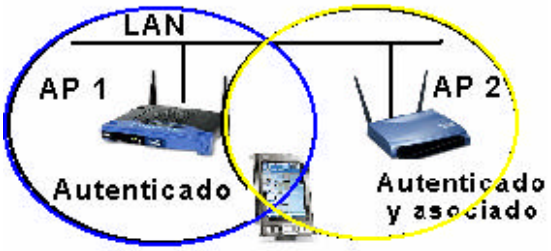

FIGURA 15: Servicio de distribución en asociación

Re-asociación
Se emplea cuando por determinas causas (roaming, modos de ahorro de energía), la estación ha perdido temporalmente la conexión con el AP y desea restaurarla para recuperar los paquetes de información que hubiesen llegado mientras tanto y que el AP los tuviese en su memoria temporal (buffer).

Des-asociación
Es el proceso empleado por el equipo para darse de baja en la celda Integración

Es la función que realiza la conversión de formatos de información entre el definido por 802.11 y el de la red a la cual está conectado el AP.

4.4 ROAMING

Se denomina roaming a la posibilidad por parte de una estación inalámbrica de desplazarse fuera de la cobertura de su celda y conectarse a otra manteniendo la continuidad de las aplicaciones que anteriormente ejecutaba.
El punto e partida lo tenemos en una estación autentificada en varios BSS y asociada a uno de ellos. A medida que se desplaza comenzara a perder nivel la señal y a partir que su valor caiga por debajo de un cierto umbral, la estación procederá automáticamente a una búsqueda de alternativas.

El primer proceso que se establece es el análisis de los diversos canales de emisión posible en busca de alternativas, proceso denominado SWEEP. Dentro de un canal determinado procede a la evaluación de la estación presente como alternativa de conexión, denominado SCANNING. Se evaluara el nivel de señal y se obtendrá el SSID de la nueva celda. Obviamente la primera condición para que se pueda producir el roaming es que nos encontremos en un sistema ESS (ambas celdas estén comunicadas entre sí por un sistema de distribución) y que las identificaciones SSID sean idénticas. El escanning puede ser de dos formas:

Pasivo
Los APs emiten periódicamente unos paquetes especiales de información denominados beacons cuya misión es la de sincronizar temporalmente a los equipos conectados e informar sobre el SSID de la celda. La estación utiliza además estos mensajes para evaluar el nivel de señal. Con esta información una nueva estación puede adoptar la decisión de conectarse.

Activo
La estación es la que emite un mensaje especial (probe) forzando a los APs dentro de su radio de cobertura y canal de emisión que respondan con un beacon.

Una vez realizado el sep entre canales y el escanning en cada uno, la estación ya puede tomar la decisión en que APs conectarse. En primer lugar recupera los paquetes de información que pudiesen haber llegado a la antigua celda e inmediatamente solicita la re-asociación a la nueva. En múltiples casos, y debido al protocolo IAPP, es necesario realizar de nuevo la autentificación. Finalmente el nuevo AP comunica al antiguo la suscripción de la estación para que elimine los datos de la misma. Todo este proceso puede llevarse a cabo cuando ambas celdas poseen un rango de direccionamiento IP en la misma subred de tal forma que el equipo mantiene la dirección IP y no se produce la interrupción de las sesiones en curso, lo cual implica que estén interconectadas a través de bridges

(nivel 2). Si los rangos son diferentes y se atraviesan routers (conectividad a nivel 3), este mecanismo no es valido y se requieren otras opciones como el establecimiento de redes privas virtuales.

4.5 ARQUITECTURAS BÁSICAS DE DESPLIEGUE INALÁMBRICO

Las arquitecturas del despliegue se pueden clasificar en: Modo punto de acceso básico, Modo con roaming y Modo de balanceo de carga.

4.5.1 Modo punto de acceso básico

Es el modo de infraestructura mas elemental en el cual un AP (pude ser un bridge o un router), está conectado a una red local y en su parte inalámbrica puede tener asociados un conjunto de estaciones. Es el modo habitual en la mayor parte de las más pequeñas instalaciones. En algunos casos se denomina modo ROOT.

4.5.2 Modo con roaming

Si se disponen de varios APs, son bridges y se configuran como una ESS con la misma SSID en todas las celdas, entonces es posible realizar el roaming de las estaciones entre ellas. Es la disposición más acertada para instalaciones de envergadura y que necesitan movilidad.

4.5.3 Modo de balanceo de carga

En zonas con elevado consumo que puede llegar a degradar e incluso saturar la capacidad de un AP, pueden desplegarse unos o mas APs en la misma ubicación y en canales de frecuencia no interferentes de tal forma que se consiga repartir el numero de estaciones y su carga entre ellos de forma dinámica. El SSID será igual en todos y se dispondrá de capacidad de roaming si son bridges. El ancho de banda será teóricamente el de un AP multiplicado por el número de ellos. Además del aumento del ancho de banda, proporciona cierto nivel de redundancia que reduce el impacto de una falta de operatividad de un AP, aunque a costa del consumo de varios canales de frecuencia.

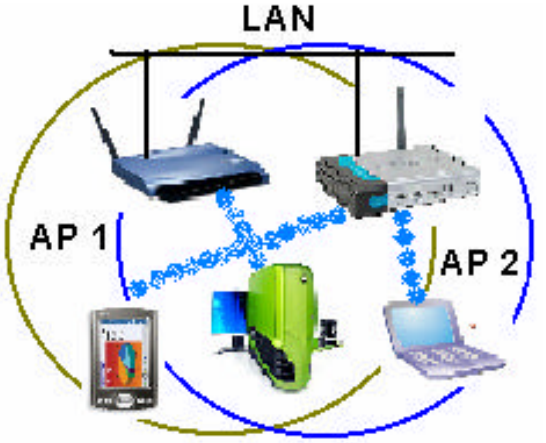

FIGURA 16: Balanceo de carga de un despliegue inalámbrico

4.5.4 Modo hot stand-by

Se configuran dos AP en la misma ubicación con diferentes parámetros y conectados a la misma red fija. Uno de ellos se pone en modo activo y el otro en stand-by en escucha permanente. En cuanto detecta que el primer AP no es operativo y toma el control de la celda. Aunque no puedan proporcionar el doble de ancho de banda de carga, solo consume un canal de frecuencia.

4.5.5 Modo repeater

Un punto de acceso se conecta a otro mediante WDS y ambos empleando el mismo canal y SSID. De esta forma el segundo AP extiende la cobertura del primero y permite que estaciones alejadas accedan a la red local cableada. Como inconveniente, se ha de indicar que se reduce muy por debajo del 50% la eficiencia del medio por necesitar enviar cada paquete de información dos veces a través del mismo canal.

4.5.6 Modo bridge

Permite conectar dos o más redes cableadas mediante un segmento inalámbrico. Uno de los bridges actúa en modo root, centralizando el tráfico, mientras que los otros adaptadores actúan como estaciones. La solución con solo dos bridges es la apropiada para enlaces punto a punto, un caso seria la interconexión entre dos edificios

4.5.7 Modo híbrido

Se configuran por la combinación de alguno de los anteriores, como por ejemplo un modo AP básico con estaciones y ala vez un bridge conectado con equipos fijos en su red cableada

5. SEGURIDAD

5.1 INTRODUCCIÓN

Hoy en día, la tecnología inalámbrica es un tema de debate de gran actualidad en el mundo empresarial. La mayoría de las organizaciones ya han implementado redes de área local inalámbricas (WLAN) o están en plena discusión sobre las ventajas e inconvenientes de esta tecnología. Son innegables las mejoras en productividad percibidas por los usuarios y el atractivo que suponen las redes de bajo mantenimiento para los departamentos de tecnología de la información (TI). No obstante, la gran preocupación por la seguridad de la mayoría de los directores de TI ha hecho que reaccionen con prudencia, si no con rotunda hostilidad, ante la idea de introducir redes WLAN en las organizaciones. Al mismo tiempo, la implementación de las soluciones propuestas por los analistas y proveedores de redes para afrontar estas preocupaciones ha parecido demasiado compleja y costosa.

5.2 REDES CABLEADAS

En las redes cableadas, la integridad de las comunicaciones dentro de nuestra red local está protegida, como la red nos pertenece físicamente, los usuarios malintencionados tendrían que invadir nuestra propiedad privada para intervenir las comunicaciones.

5.3 REDES INALÁMBRICAS

Por su naturaleza nuestros datos viajan por el espectro radioeléctrico, no se encuentran confinados en ningún medio físico, por lo tanto llegarán a todos los puntos donde alcance la cobertura de la señal, en el caso de una red wifi típica, de un radio de entre 10-100 mts, las señales se emiten en bandas del espectro públicas (de libre acceso) y buscar actividad radioeléctrica es una actividad lícita.

Despliegue

una gran parte del equipamiento wi-fi y de las aplicaciones que lo acompañan ha sido diseñado con el objetivo de facilitar al máximo el despliegue de una red de este tipo, los APs pueden utilizarse directamente con la configuración de fábrica, en opciones como: Aplicaciones de configuración gráficas y vía web, canal 5 o 6 de la banda de frecuencias, SID (identificador de red) por defecto del fabricante,

transmisiones de hasta 11mbps con adaptación de la tasa binaria antena omnidireccional (emite en todas las direcciones con igual potencia).
La configuración de fábrica de las tarjetas inalámbricas, del mismo fabricante que los APs que se estén utilizando, permite el uso de esta red directamente, cualquiera con una tarjeta de ese fabricante pueden conectarse a nuestra red. Esta enorme facilidad en la instalación y el despliegue beneficia la expansión e implantación de esta tecnología a todos los niveles.

Problemas de seguridad

El funcionamiento de las tarjetas inalámbricas Wi-Fi favorece:
La sencillez del despliegue, los problemas de seguridad provenientes de: configuraciones por defecto, desconocimiento de las características del equipamiento, desconocimiento de los mecanismos de seguridad.

El propio driver de las tarjetas muestra al usuario un resumen con todas las redes Alcanzables: BSSID (dirección MAC) de los APs alcanzables, SSID (identificador) de la red a la que pertenece cada AP, Canal en el que está emitiendo el AP

Esta información mostrada, en el modo de funcionamiento más básico de una red Wi-Fi, es todo lo que necesitamos para poder conectarnos a ella. Hay herramientas públicas (NetStumbler o Airsnort), utilizadas casi en la misma proporción por los
Administradores de red y usuarios malintencionados, especializadas en mostrar la información de todas las redes alcanzables y vulnerables. En la grafica se muestra un ataque común desde un parqueadero o un lugar cerca de nuestra red.
En la grafica muestra los beneficios que el atacante puede tener

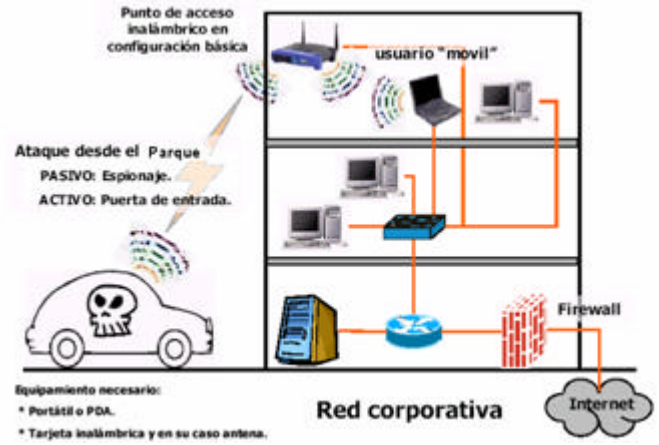

FIGURA 17: Ataque desde el parqueadero en una red inalámbrica

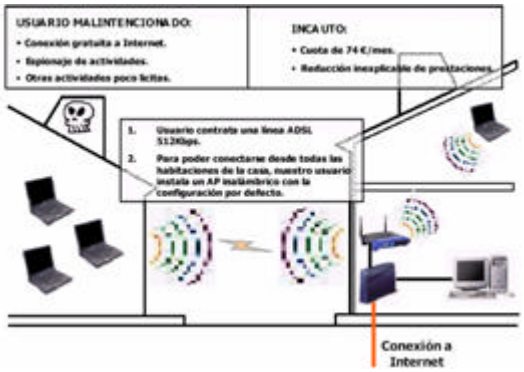

FIGURA 18: Beneficios de un atacante en una red inalámbrica

5.4 FASES DE UNA CONEXIÓN INALÁMBRICA WIFI

Fase 1y 2 rastreo de frecuencia

El equipo móvil inalámbrico escánea el espectro radioeléctrico en busca de actividad, rastrea automáticamente todos los canales en busca de puntos de acceso disponibles, envía peticiones y espera la recepción de anuncios por parte de los APs.

Los APs, en su modo de funcionamiento por defecto, generan tramas de gestión (Beacon Frames), en las que envían el SSID (Service Set Identifier) de la red a la que pertenecen, esto se presenta periódicamente (Ap Beacon Frame), y en respuesta a una petición de los posibles clientes (Probe Request, Probe Response).
El SSID se utiliza para diferenciar entre distintas redes. Bajo la cobertura de APs con el mismo SSID pertenecientes a la misma red (misma dirección IP, misma mascara, misma puerta de enlace,), WI-FI soporta la itinerancia de los clientes.
Un cliente que se conecte a través de uno de los APs de la red y obtenga por DHCP una dirección, podrá desplazarse al rango de cobertura de otro AP de la misma red manteniendo la conectividad.

En el equipo móvil se muestra al usuario un resumen con las redes alcanzables por razones de cobertura, aquí aparece, normalmente, solo el AP del que se recibe una mayor intensidad de señal

Fase 3. Proceso de autentificación del cliente.

El cliente envía una petición de autentificación al AP elegido en la fase anterior, En función de los métodos implementados por los administradores de red se Autenticará al cliente mediante alguno de los siguientes métodos:

Autentificación en base al SSID del cliente: el AP comprueba que el SSID que envía el cliente en sus tramas corresponda con el suyo.

Autentificación en base a la dirección MAC del cliente: el AP mantiene una lista de direcciones MAC admitidas.

Autentificación basada en retos mediante encriptación WEP.

Fase 4. Asociación y transferencia de datos

El cliente inalámbrico, en caso de finalizar correctamente la fase anterior, se asocia con el punto de acceso, A partir de ahora el equipo inalámbrico móvil puede comenzar la transferencia de datos, Con otros equipos inalámbricos incluidos en el rango de cobertura del punto de acceso Y Con otros equipos incluidos en la parte cableada de la red.

5.5 WEP (Wireless Equivalent Protocol)

La seguridad WEP se basa en un mero secreto compartido (clave o contraseña) para la autenticación en la WLAN. Todo el que posea esta dave secreta podrá contar con acceso a la WLAN. La WEP estándar original no proporciona ningún método para automatizar la actualización o distribución de estas claves; por lo tanto, resulta extremadamente difícil cambiarlas con regularidad. Los defectos de cifrado en la WEP implican que un atacante puede descubrir las claves WEP estáticas mediante herramientas sencillas. Por estas razones este estandar a entrado en decadencia

Características

Se basa en el algoritmo RC4 desarrollado por RSA Systems. Algoritmo de clave simétrica, Las dos partes de la comunicación (emisor y receptor) comparten un secreto, una clave común, con la que encriptan/desencriptan
Las comunicaciones se encuentran en Versiones con claves de 64 y 128 bits.
Fija el mecanismo mediante el cual se autentica al grupo de usuarios al que se le permite acceder a la red, por lo tanto No autentifica usuarios individuales, tampoco autentifica a los puntos de acceso.
Fija el mecanismo mediante el cual se encriptan/desencriptan los datos transportados en la trama MAC.
No fija ningún mecanismo de determinación ni distribución de claves.

Llaves

La llave de 40 ó 104 bits, se genera a partir de una clave (passphrase) estática de forma automática, aunque existe software que permite introducir esta llave manualmente.
La clave o passphrase debe ser conocida por todos los clientes que quieran conectarse a la red wireless que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente.
A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.
Este es el proceso que se realiza para generar las llaves:

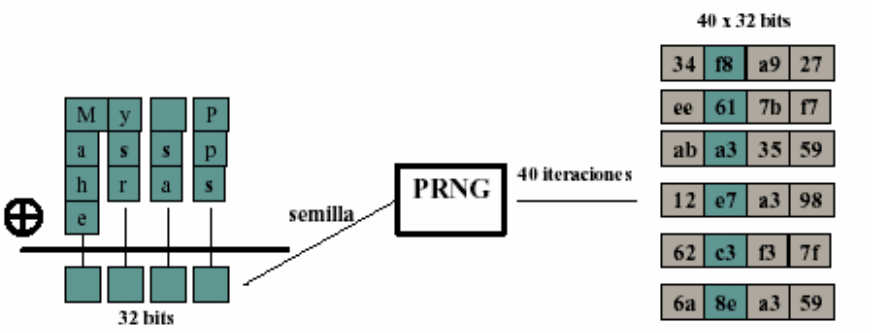

FIGURA 19: Llave en una WEP

Se hace una operación XOR con la cadena ASCII (*My Passphrase*) que queda transformada en una semilla de 32 bits que utilizará el generador de números pseudo aleatorios (PRNG) para generar 40 cadenas de 32 bits cada una.
Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits. De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP

5.5.1 Encriptado de datos

Trama encriptada con wep

Para generar una trama encriptada con WEP se sigue el siguiente proceso:

Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene unos datos (Payload). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como valor de chequeo de integridad (ICV: Integrity Check Value):

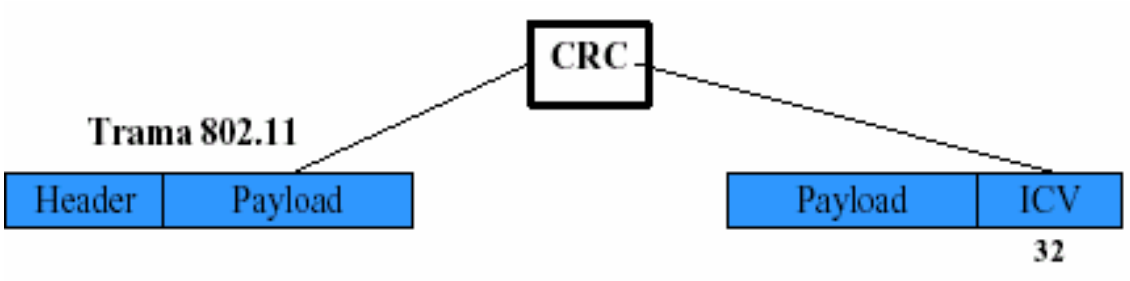

FIGURA 20: Trama encriptada con WEP (1)

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles:

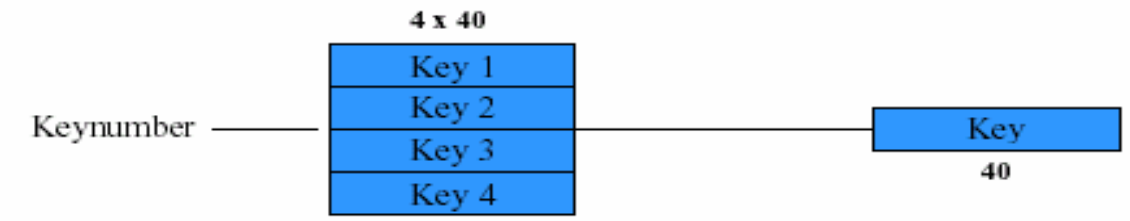

FIGURA 21: Trama encriptada con WEP (2)

Y añadimos el Vector de Inicialización (IV) de 24 bits al principio de la llave Seleccionada:

FIGURA 22: Trama encriptada con WEP (3)

El IV es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero.
Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128 bits tendríamos 24 bits de IV y 104 de llave.
Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV + Key y conseguiremos el keystream o flujo de llave. Realizando una operación XOR con este keystream y el conjunto Payload+ICV obtendremos el Payload+ICV cifrado, este proceso puede verse en el siguiente grafico.

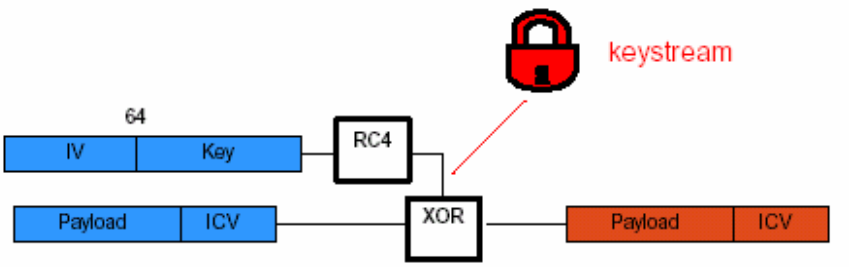

FIGURA 23: Trama encriptada con WEP (4)

Después añadimos la cabecera y el IV+Keynumber sin cifrar. Así queda la trama definitiva lista para ser enviada:

FIGURA 24: Trama encriptada con WEP (5)

El proceso de encriptación en conjunto se ve resumido en este esquema:

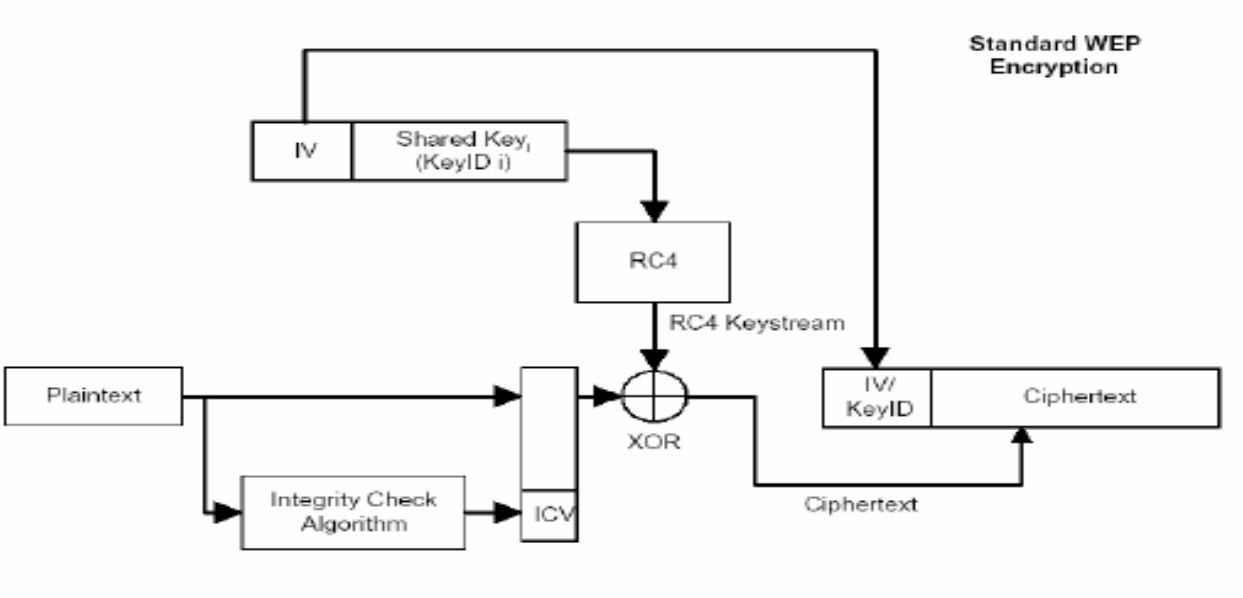

FIGURA 25: Esquema general del proceso de Encriptación

5.5.2 Desencriptado de datos

Se utiliza el número de llave que aparece en claro en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama:

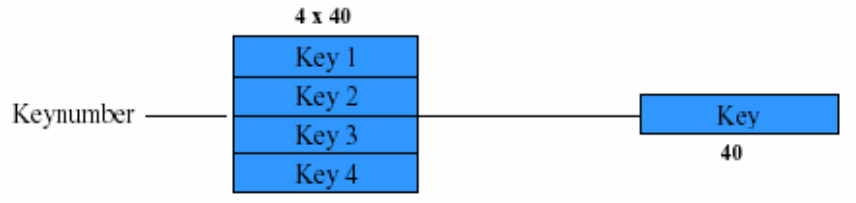

FIGURA 26: Proceso de desencriptados de datos (1)

Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave obtenemos el keystream válido para obtener la trama en claro (plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa como se describe a continuación.

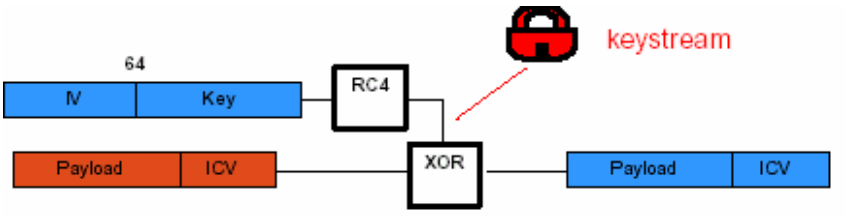

FIGURA 27: Proceso de desencriptados de datos (2)

Una vez obtenido el plaintext, se vuelve a calcular el ICV del payload obtenido y se compara con el original. El proceso completo puede verse en el siguiente esquema:

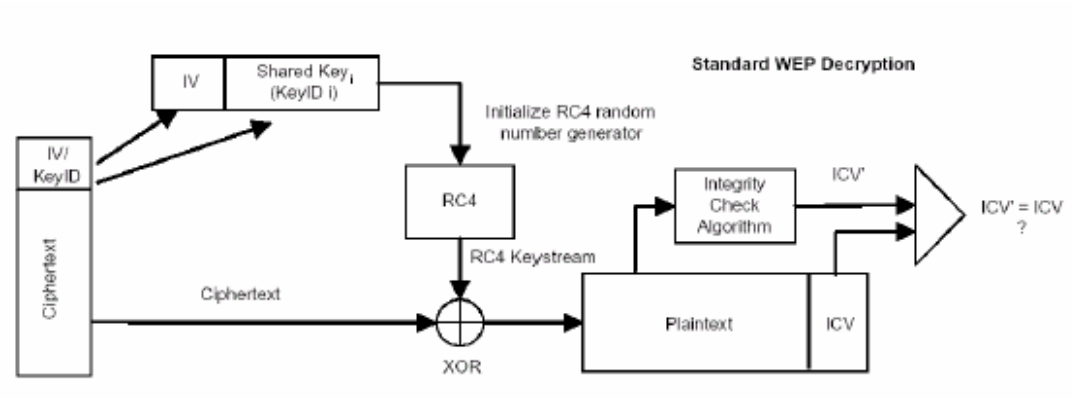

FIGURA 28: Esquema general de proceso de desencriptación

5.5.3 Mecanismos de autentificación de usuarios

Open system authentication

Es el protocolo de autenticación por defecto para 802.11b.
Como su nombre indica, este método autentica a cualquier cliente que pide ser autenticado. Es un proceso de autenticación NULO, las tramas se mandan en texto plano aunque esté activado el cifrado WEP.

Shared Key Authentication

Este mecanismo utiliza una clave secreta compartida, que conocen cliente y AP.

FIGURA 29: Mecanismo shared key de autenticación

La estación que quiere autenticarse (cliente), envía una trama Authentication Request indicando que quiere utilizar una "clave compartida". El destinatario (AP) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente.
El texto del desafío se genera utilizando el PRNG (generador de números pseudoaleatorios de WEP) con la clave compartida y un vector de inicialización (IV) aleatorio.
Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el payload de una nueva trama, que encripta con WEP utilizando la clave compartida (*passphrase*) y añade un nuevo IV (elegido por el cliente). Una vez construida esta nueva trama encriptada, el cliente la envía al AP, y éste desencripta la trama recibida y comprueba que:
El ICV (Integrity Check Value) sea valido (CRC de 32 bits).

El texto de desafío concuerde con el enviado en el primer mensaje.

Si la comprobación es correcta, se produce la autenticación del cliente con el AP y entonces se vuelve a repetir el proceso pero esta vez el primero que manda la trama con el AUTHENTICATION REQUEST es el AP. De esta manera se asegura una autenticación mutua.

5.5.4 Problemas de los mecanismos básicos de seguridad

El SSID, ya que es un identificador de red y sirve para diferenciar distintas redes inalámbricas, en los primeros despliegues de redes IEEE 802.11b era utilizado como una especie de passwordde acceso.
Los administradores lo utilizaban para diferenciar a los usuarios autorizados de los que no poseían permiso.

Problemas:

Los APs, en su configuración por defecto, transmiten en claro en ciertas tramas de gestión el SSID cada 10ms:
Facilita el procedimiento de descubrir nuevas redes y puntos de acceso.
Permite que cualquier usuario equipado con una tarjeta IEEE 802.11 y el driver de la tarjeta pueda descubrir nuestra red y hacerse con el SSID.

Hay tarjetas que admiten como SSID

El SSID solo sirve para evitar asociaciones accidentales con APs pertenecientes a otras redes.

El broadcast del SSID en los mensajes de anuncio de la red puede deshabilitarse: Sigue viajando en claro en las respuestas desde el AP.

Autentificación en base a las direcciones MAC

Los APs guardan listas de direcciones MAC admitidas.
Si la dirección MAC de la trama está en la lista el cliente puede continuar con la autenticación y la asociación.

La cabecera de las tramas MAC siempre viaja en claro por el espectro electromagnético.
Con un equipo IEEE 802.11 y un programa adecuado (Ethereal, tcpdump) podemos ponernos a la escucha de paquetes (sniffing) esperando a ver una comunicación entre un AP y un cliente admitido. Una vez analizado los paquetes el usuario malintencionado puede ocultar su dirección MAC real tras esta nueva dirección MAC admitida, proceso conocido como spoofing, de forma sencilla.

Paquetes software como SMAC (KLC Consulting, Inc) permiten el cambio software de la dirección MAC en los paquetes sin manipular la dirección hardware real de los dispositivos.
Algunas versiones realizan el cambio de dirección MAC a una permitida de forma automática. Script kids

FIGURA 30: Procedimiento de spoofing de la dirección MAC

Encriptación de datos con WEP

Dos paquetes encriptados con la misma clave WEP, en los que se repita el vector IV, provocan que un atacante pueda extraer la clave WEP.
Hay programas (WEPCrack, AirSnort que obtienen la clave WEP.
Diversos estudios afirman que con 1GByte de información intercambiada entre el AP y los clientes esta clave IV se repite.

FIGURA 31: Ataque en la Encriptación de datos con WEP

5.6 WPA (WiFi Protected Access)

Introducción

IEEE trabajo en un estándar de seguridad para las WLAN denominado 802.11i; también conocido como "red de seguridad sólida" (RSN). La Alianza Wi-Fi, un consorcio formado por proveedores de fidelidad inalámbrica (Wi-Fi), publico un estándar del sector denominado "Acceso protegido Wi-Fi" (WPA) lo que es, básicamente, una versión previa del 802.11i. WPA incluye un amplio subconjunto de funciones de 802.11i. Al publicar el WPA, la Alianza Wi-Fi ha podido exigir la adherencia a la WPA de todos los equipos que lleven el logotipo Wi-Fi y ha permitido que los proveedores de hardware de redes de Wi-Fi ofrezcan una opción de alta seguridad estandarizada con anterioridad a la publicación del 802.11i. WPA reúne un conjunto de características de seguridad ampliamente aceptadas como las técnicas disponibles para proteger las WLAN.

Modos de operación de WPA

WPA incluye dos modos: uno, que emplea 802.1X y la autenticación RADIUS (conocida simplemente como WPA) y otro esquema más sencillo para entornos SOHO que emplea una clave compartida previamente (conocida como WPA PSK). WPA asocia el cifrado seguro con la autenticación fuerte y el mecanismo de autorización de 802.1X. La protección de datos de WPA elimina las vulnerabilidades conocidas de WEP con los siguientes métodos:

Utilización de una clave de cifrado única para cada paquete.

Utilización de un vector de inicialización mucho más largo, duplicando de forma eficaz el espacio de clave al agregar 128 bits adicionales de material para claves.

Adición de un valor de comprobación de integridad de mensaje firmado que no sea vulnerable a la alteración de datos o la suplantación

Incorporación de un contador de marcos cifrado para impedir los ataques de reproducción

No obstante, dado que WPA utiliza algoritmos criptográficos similares a los empleados por WEP, se puede implementar en el hardware existente con una sencilla actualización de firmware.

El modo PSK de WPA también permite que las pequeñas organizaciones y los trabajadores domésticos utilicen una WLAN de clave compartida carente de las

vulnerabilidades de la WEP estática (siempre que la clave compartida previamente que se haya elegido sea lo bastante segura como para evitar meros ataques de adivinación de contraseña). Al igual que la WEP dinámica y el WPA basado en RADIUS, las claves de cifrado individuales se generan para cada cliente inalámbrico. La clave que se ha compartido previamente se emplea como una credencial de autenticación; si dispone de esa clave, entonces tendrá autorización para emplear la WLAN y recibir una clave de cifrado exclusiva con el fin de proteger los datos.
Define 3 tipos de entidades:

Solicitante: es el cliente inalámbrico

Autentificador: actúa como intermediario entre el cliente inalámbrico y el servidor de autentificación, en un escenario común, será el punto de acceso

Servidor de autentificación: sistema de autentificación que guarda la información relacionada con los usuarios y las autentificaciones activas.

FIGURA 32: Entidades para la clave de cifrado

Proceso de autentificación

1. El solicitante, un cliente inalámbrico que quiere ser autenticado, envía una petición al autentificador.

2. El autentificador, punto de acceso, habilita un puerto para el solicitante, por este puerto solo pueden viajar mensajes de autentificación en tramas de gestión, el resto del tráfico se filtra (DHCP, HTTP, FTP, SNMP, POP3).

3. El autentificador pide la identidad al solicitante mediante el protocolo EAPOL (EAP Encapsulation Over LANs).

4. El solicitante envía su identidad al autentificador.

5. El punto de acceso envía la identidad del cliente al servidor de autentificación mediante EAP (Extensible Authenti cation Protocol).

6. El cliente y el servidor de autentificación establecen un diálogo mediante el protocolo EAP, finalizado este diálogo, el solicitante y el servidor de autentificación comparten una clave de sesión que nunca ha viajado por la red.

7. El servidor de autentificación envía la clave de sesión al autentificador mediante el protocolo RADIUS.

8. El punto de acceso habilita el puerto para la dirección MAC del dispositivo solicitante y adicionalmente establece una clave de encriptación con el solicitante.

TKIP (Temporal Key Integrity Protocol)

Se basa en el algoritmo RC4 pero: Con vector de inicialización (IV) de 48 bits presenta Claves distintas y dinámicas para cada usuario requiere Una clave diferente para cada paquete enviado.

Posee dos tipos de claves: Unicast y Broadcast

Unicast:
Pairwise Master Key (PMK): Acordada por el solicitante y el servidor.
Pairwise Transient Key (PTK): Derivada de la PMK mediante mezclado con las direcciones MAC de soliitante y el autentificador y el Temporal Key (TK). Para encriptar los mensajes de datos.

Broadcast:
Groupwise Master Key (GMK): Para poder enviar mensajes multidestino, distribuido desde el AP (autentificador) a los clientes (solicitante), cada AP puede tener una diferente.

Distribución de claves mediante 4-way handshake y group key handshake.

Clave única por paquete (PPK)

La clave se modifica con el envío de cada paquete psee una clave inicial, particularizada para cada cliente con su dirección MAC, se mezcla con el vector IV, este se modifica con cada envío. (PPK. Perpacket Keying) y está relacionado con el número de secuencia del paquete.

Para evitar la posibilidad de colisión de dos paquetes, uno desde el AP y otro desde el cliente IV, encriptados con la misma clave y el mismo vector de inicialización el Cliente precenta una numeración impar y el AP numeración par.

5.7 REDES PRIVADAS VIRTUALES (VPN)

VPN es una solución excelente para atravesar una red hostil como Internet (aunque la calidad de las implementaciones de VPN varíe). Sin embargo, no es necesariamente la mejor solución para asegurar las WLAN internas. Para este tipo de aplicaciones, una VPN ofrece poca o ninguna seguridad adicional en comparación con las soluciones 802.1X; al mismo tiempo que incrementan de manera significativa la complejidad y los costes, reducen el aprovechamiento y hacen que partes importantes de las funciones no estén operativas

Ventajas de utilizar VPN en WLAN:

La mayoría de las organizaciones ya han implementado una solución de VPN, así que tanto los usuarios como el personal de TI estarán familiarizados con la solución.

La protección de los datos de la VPN suele emplear el cifrado de software que permite que los algoritmos se modifiquen y se actualicen con mayor facilidad que el cifrado basado en el hardware.

Es posible utilizar hardware relativamente menos costoso porque la protección de VPN es independiente del hardware de WLAN (aunque el aumento de precio que conlleva el hardware de red apto para 802.1X no ha desaparecido en absoluto).

Inconvenientes de utilizar VPN

Las VPN carecen de transparencia para el usuario, los clientes VPN inician manualmente una conexión con el servidor de VPN. Si la VPN se desconecta, debido a una señal de WLAN escasa o como consecuencia de que el cliente se esté moviendo entre los puntos de acceso, el usuario deberá volver a conectarse.

Un equipo no se puede administrar o supervisar remotamente a menos que un usuario inicie la sesión.

Si se reanuda desde un estado de espera o hibernación, la conexión de VPN no se volverá a establecer de forma automática, sino que el usuario deberá hacerlo manualmente.

Aunque los datos del interior del túnel VPN están protegidos, la VPN no ofrece protección para la propia WLAN. Un intruso podría seguir conectado a la WLAN e intentar sondear o atacar dispositivos conectados a la WLAN.

El coste del servidor VPN y de las licencias de software del cliente, así como el coste de implementar el software, pueden constituir un problema en el caso de soluciones de VPN

Aunque el tráfico que pasa a través de la VPN esté protegido, la infraestructura inalámbrica sigue comprometida. Un usuario que consiga el SSID, una MAC permitida y la clave WEP podrá utilizar la red inalámbrica salvo que el AP solo permita el paso de tráfico de VPN autenticado.

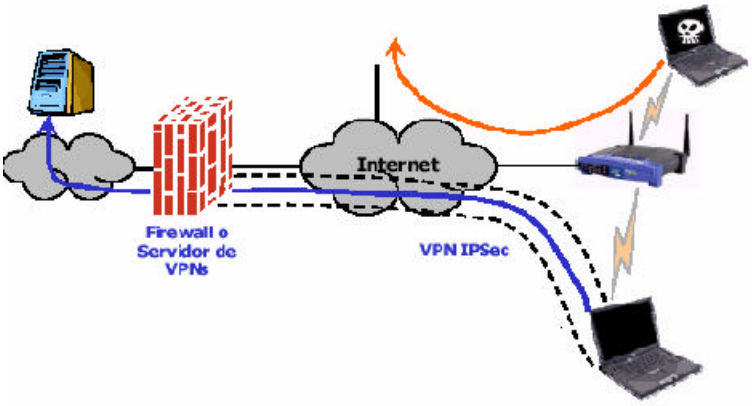

FIGURA 33: Ataque en una VPN inalámbrica

5.8 WPA 2

Nuevo estándar de seguridad para redes inalámbricas.

Posiblemente no sea compatible con el equipamiento antiguo, no es suficiente con una actualización de firmware presenta mas más potencia de cálculo, requiere coprocesador.

Modos duales: WPA/WEP y WPA2/WPA.
Soporte para itinerancia rápida un Usuario pre-autenticado contra todos los puntos de acceso cercanos no solo con el que esta asociado.

Encriptación AES (Advanced Encryption System):
Algoritmo de Rijndael.
Sustituye a DES y 3DES, típicos en la encriptación de VPNs y las comunicaciones bancarias.
Aprobado por el NIST (National Institute of Standars).
Resistente a todos los ataques de criptoanálisis conocidos.

6. IMPLEMENTACIÓN DE REDES INALÁMBRICAS EN UNIVERSIDADES

6.1 NORMAS QUE SE DEBEN SEGUIR

Para implementar redes inalámbricas en las universidades se debe seguir varias normas, para que red sea lo mas optima posible, para eso se deben cumplir unos parámetros básicos en cuanto a cobertura, diseño y calidad de nuestra red, entre otros. A continuación se mostrara todo el despliegue técnico y se darán recomendaciones para la escogencia de la mejor red

La planificación es una parte importante en este proyecto con lo que respecta a lo que sabemos y necesitamos. Algunos aspectos importantes para tener en cuenta

1. Una gran fracción del equipamiento WiFi puede considerarse Plug and Play esto quiere decir que Con la configuración de fábrica podemos obtener una red básica formada por un AP y los clientes inalámbricos, únicamente con conectar cable Ethernet al APs, alimentar AP e instalar físicamente la tarjeta inalámbrica en los PC de los estudiantes.

2. Si pretendemos extender sin más esta configuración a una infraestructura más Complicada, con varios APs, aparecen problemas de interferencia destructiva. lo que representa una caída de hasta el 50% del ancho de banda si los APs están demasiado cerca en la tabla se observa los distintos escenarios que se pueden presentar cuando hay puntos de acceso cercanos y los valores que se decrementán

3. Si intentáramos colocar nuestra red de un modo plug and play estaríamos ignorando totalmente uno de los aspectos principales a tener en cuenta en un despliegue inalámbrico, la seguridad, por lo tanto tendríamos una red sin autentificación, sin encriptación de datos, y con accesibilidad a cualquier persona que disponga de un equipo WiFi.

Configuración de los Aps (sintonización de canales)	Prestaciones por cliente (tráfico ftp desde servidor en red FastEthernet)
1 solo cliente por AP **5** canales o más de distancia	Aproximadamente **4.8Mbps** cada cliente
1 solo cliente por AP **4** canales de distancia	Aproximadamente **4Mbps** cada cliente
1 solo cliente por AP **3** canales de distancia	Aproximadamente **3.5Mbps** cada cliente
1 solo cliente por AP **2** canales de distancia	Aproximadamente **3Mbps** cada cliente
1 solo cliente por AP **1** canal de distancia	Aproximadamente **2.8Mbps** cada cliente
1 solo cliente por AP Los 2 APs en el mismo canal	Aproximadamente **2.5Mbps** cada cliente

TABLA 4: Configuración de los APs Vs prestaciones por cliente

La cobertura incontrolada es otro factor que se debe tener en cuenta. Al momento de configurar y asignar el ancho de banda en las diferentes zonas, se debe hacer un estudio predeterminado en el cual, la demanda de ancho de banda que se pueda presentar debe satisfacer en todo momento, lo cual no amerita que se deba abonar mas ancho de banda en un sector que no se muy utilizado.

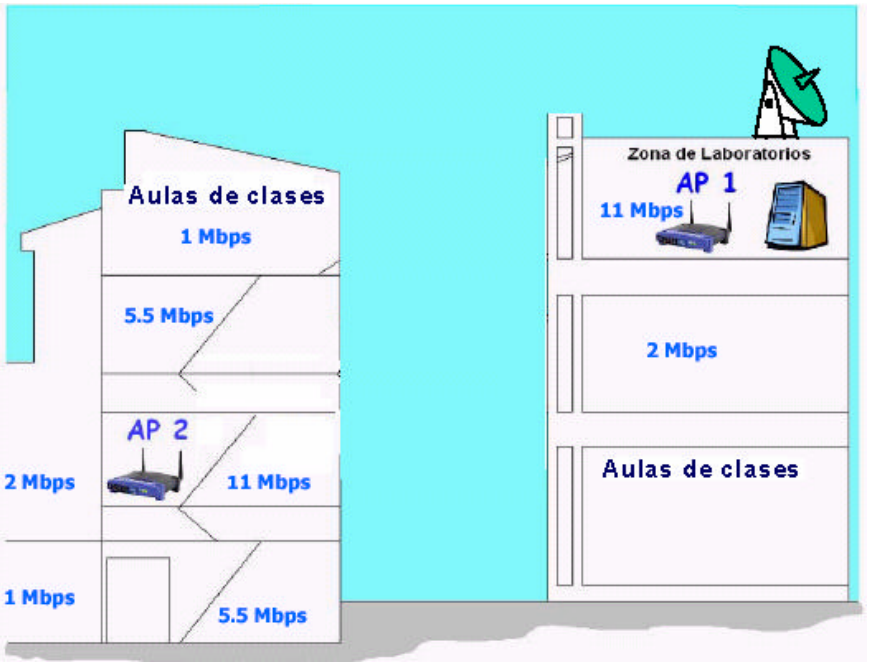

FIGURA 34: Cobertura incontrolada

4. otras dificultades comunes podrían ser:

Sistemas de interiores en exteriores: Los sistemas de interiores tiene bajas tolerancias. Si se sitúan directamente en exteriores o en semi-exteriores (patios internos) acababan averiándose ya que la propia circuitería genera variaciones de temperatura que acaban provocando condensación de agua en su interior. Por lo tato con el fin de abaratar costos se utilizan estos métodos lo que puede ocasionar grandes pérdidas en el futuro.

Sistemas de interiores en interior con antena en el exterior: hay que tener en cuenta que muchos instaladores de red optan por instalar el sistema en el interior, pero como la antena debe estar en el exterior se ven obligados a utilizar largos cables de conexión entre los sistemas y sus antenas. La longitud del cable de antena es crítica ya que conlleva pérdidas. Las instalaciones con cables largos de antena dan unos niveles de cobertura muy pobres a menos que se utilicen amplificadores, pero el uso de amplificadores (caros) ya desvirtúa la única ventaja de los sistemas para interiores, el precio, y se complica la instalación y se aumentan las necesidades de mantenimiento.

6.2 ASPECTOS PRÁCTICOS EN DESPLIEGUE DE LA RED INALÁMBRICA

Cuando se quiera implementar un diseño en un distinto escenario universitario, se deben seguir ciertos parámetros y aspectos que serán fundamentales en la ubicación e implementación de nuestra red, estos aspectos son:

Evaluación de los objetivos.
Elección del equipamiento adecuado.
Evaluación de la cobertura.
Selección y sintonización de canales.
Implantación de medidas de seguridad**.**

6.2.1 Evaluación de los objetivos

Lo primero que debemos tener en cuenta al momento de realizar el proyecto es evaluar y tener claro todos los objetivos que se planteen.

1. Tipo de red

Como nuestro escenario va ha ser las distintas universidades que quieran emigrar a esta tecnología, el tipo de red adecuada será una red corporativa puesto que estas redes su principal parámetro es la seguridad, que es un aspecto fundamental en el despliegue. Dentro de la red corporativa la mas adecuada será una red híbrida puesto que se cuenta en la mayoría de los casos una red cableada existente en la universidad, esto nos va ha permitir abaratar costos en nuestro proyecto

2. Lugar del despliegue
Este es un objetivo primordial en el desarrollo de la red inalámbrica puesto que se deben tener en cuenta ciertos parámetros que serán transcendentales cuando deseemos montar la infraestructura como son:

Los tipos de obstáculos que sortearemos en nuestro despliegue. Madera, plástico, ladrillos, mármol, materiales sintéticos que en cierto punto producirán una atenuación a la señal.

Más redes inalámbricas en el mismo espacio, debemos hacer un estudio general de la zona donde nos encontremos, para saber si las redes inalámbricas que podemos encontrar cerca de la nuestra, pueda interferir en un funcionamiento optimo.

Focos de interferencias, aunque la tecnología WI-FI trabaja a una frecuencia determinada, se debe hacer un estudio de frecuencia que se este utilizando en la zona, como por ejemplo, el uso e teléfonos inalámbricos trabaja la misma frecuencia de la tecnología, se observa el canal que este trabajando dicho teléfono y se escoge un canal distinto para la implementación de nuestra red. Recordemos que WI-FI dispone de 10 canales diferentes en una frecuencia determinada

3. Tipos de usuarios.
Antes de ubicar el número de canales disponible en alguna zona especificar es importante tener en cuenta que tipos de usuarios se movilizaran por dicha zona. Estos usuarios pueden se:

Estáticos: usuario que siempre estará en el mismo lugar o misma zona, este tipo de usuarios se podrían encontrar en la biblioteca, o en salones que ya tengan un equipo predeterminado.

Semiestáticos: son alumnos que caminan de un lugar a otro pero que se pueden encontrar dentro de la cobertura que da el punto de acceso. Podría ser el caso de la zona de cafetería

Itinerantes: son usuarios que por su movilidad pueden pasar de una zona de cobertura de un punto de acceso a otra. Aquí es importante que el dispositivo o punto de acceso que se utiliza tenga la capacidad de hacer roaming

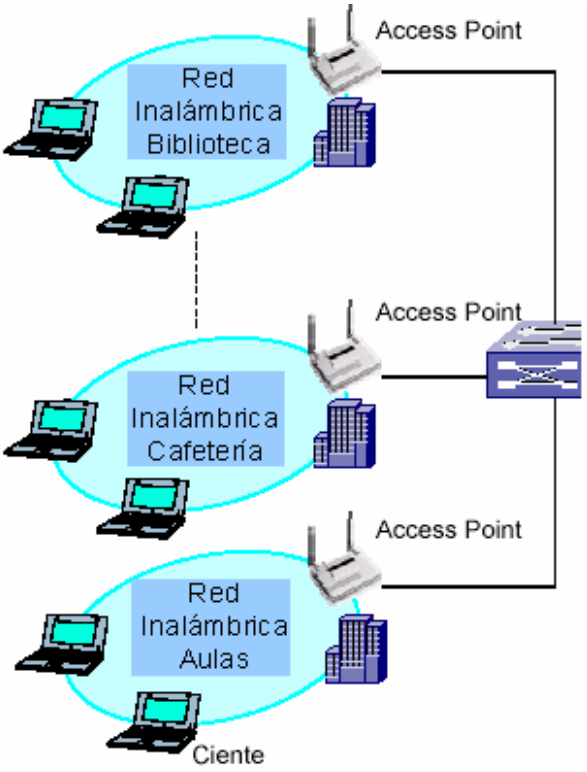

FIGURA 35: Lugares de despliegue

5. Prestaciones necesarias por usuario.

Se deben escoger zonas especifica donde la necesidad del usuario se satisfaga, habrán zonas donde el requerimiento de ancho de banda es mayor que en otras, por circunstancias que pueden ser, acceso a Internet, transferencia de archivos, videoconferencia. A estas zonas se tiene que configurar el punto de acceso para asignar un ancho de banda mayor.
El ancho de banda total, efectivo, disponible en un canal dado en el que no se sufra interferencias se encuentra alrededor del 50% del ancho de banda ofrecido por cada modulación dada.

El acceso al medio es por contienda:
Si el número de usuarios n es muy elevado, cada usuario verá un ancho de banda menor que la enésima parte del total. 20-25 usuarios, 100Kbps mínimo por usuario por AP.

Es muy importante tener en cuenta el número de usuarios que vamos a soportar de cara a dimensionar adecuadamente la conexión de nuestra red al exterior, para

determinar el numero de usuarios que puedan conectarse a bs determinados punto de acceso debemos identifica que clase usuario se encuentra en dicha zona, además la cobertura que dispone nuestro punto de acceso, las interferencias en el medio. Esto nos ayudara a saber la capacidad de nuestra red.
25 usuarios x100kbps mínimo =2,5 Mbps de BW de salida a Internet.

FIGURA 36: Limitación de prestaciones para el usuario

6.2.2 Elección del equipamiento adecuado

1. Línea de productos
Dentro de los diferentes productos que se encuentran en el mercado existe una gran variedad des gamas para escoger, es indispensable que se elija una gama alta de producto, puesto que sus especificaciones y parámetros serán los adecuados para la red que se quiera implementar. Para la opción de gama baja estas se aplican para redes pequeñas de oficina o del hogar por eso no son especificadas dentro de este documento
Los productos de gama alta tienen las siguientes características:
Presentan Múltiples medios de acceso y la configuración del equipo es variada (ssh, NMP, puerto de consola local).

Están diseñados para garantizar en lo posible la integridad de la infraestructura de red y de las comunicaciones que la atraviesan. Por lo general presentan una Configuración "áspera"

Poseen Múltiples opciones de configuración, como direccionalidad de las antenas, control de potencia emitida, designación de ancho de banda por usuario y por zona

2. Tipos de equipos a los que se va a dar acceso a la red
Aquí se nombraran los equipos comunes en las redes inalámbricas para las universidades:

Equipos fijos (PC de sobremesa): se supone que la universidad que se vaya a implementar esta tecnología ya posee computadores dentro de sus activos, por lo que únicamente tiene que adquirir los accesorios necesarios para la conexión a la red, como son: Tarjeta USB, Tarjeta PCI, Si poseen bahía PCI tarjeta PCMCIA.

Equipos portátiles: como la mayoría de estudiantes no cuenta con esta clase de equipos se recomienda a las universidades que quieran implantar este sistema, realizar un consorcio con una empresa de computadores para adquirir los aparatos a bajo costo, y con un plan de cuotas fijas brindarle al estudiante la posibilidad de tener su computador portable desde un cierto nivel académico, actualmente la mayorías de portatilies ya traen soporte para WiFi integrado.

Equipos móviles (PDA): aquí en Colombia estos dispositivos son muy pocos utilizados a nivel de estudiante universitario sin embargo cada vez están más extendidos y pronto serán parte indispensable de nuestro trabajo o vida personal. Sus crecientes capacidades gráficas, potencia y memoria facilitará el uso de navegadores y por tanto la ejecución de aplicaciones avanzadas, Las últimas versiones traen soporte para WiFi integrado.

3. Funcionalidades que debe ofrecer la red inalámbrica:

Punto de acceso:
Es el principal dispositivo que tendremos en la red por eso su escogencia debe ser muy cuidadosa, no es necesario poner puntos de acceso con las mismas características en diferentes zonas, estos pueden variar de acuerdo a las necesidades.

Router inalámbrico:
Suele situarse justo como el siguiente equipo al modem en una conexión a Internet por eso es fundamental si necesitáramos un router en nuestra conexión presentara las siguientes características:
Que posea mínimo 1 interfaz para conectar al modem, Una serie de interfaces para conectar equipamiento cableado, Interfaz IEEE 802.11y que presente otras funcionalidades como, Servidor DHCP incorporado, NAT y PAT automático, Adquisición de la dirección IP automática en su interfaz pública.

4. Las antenas con las que vienen equipados los AP, los routers inalámbricos, las tarjetas inalámbricas, son por lo general omnidireccionales. Por lo facilitan el descubrimiento de nuevas redes, además los equipos móviles poseen poca sensibilidad para reducir el consumo de potencia.

5. Puede ser necesario realizar un enlace punto a punto, Unir dos edificios cercanos de la misma universidad para esto se recomienda, crear un núcleo de

red inalámbrico (Zamora Hot City). Con este enlace y dependiendo la marca del fabricante se pueden conectar edificios separados hasta de 40 Km, con retorno de inversión y un ancho de banda comparable al de una línea T1, (ver anexo 1).

6. Una parte del equipamiento WiFi permite modificar el diagrama de radiación de la antena de omnidireccional a semicircular.

7. Otros equipos permiten el cambio de la antena de fábrica a otra más adecuada a nuestros objetivos, como son las antenas direccionales.

6.2.3 Evaluación de la cobertura.

Existe bastante confusión acerca de cómo instalar coberturas inalámbricas en varias plantas. Por lo general, se tiende a pensar que un punto de acceso con una antena muy potente sería suficiente para dar cobertura a todo el edificio. Esto no es así, a menos que sea una universidad de pocas plantas, y la cobertura en cada planta podría no ser homogénea.
Cuando se afronta este tipo de instalaciones debemos pensar bien la infraestructura.

De cara a posicionar un AP en nuestra red es obligatorio evaluar siempre el rango de cobertura para esto se debe:

Minimizar las zonas en las que damos cobertura sin desearlo. Se podrá hacer un cambio del diagrama de radiación de la antena y se llevara un control de la potencia emitida.

Observar los efectos que tienen sobre el área de cobertura los obstáculos, se realizara un estudio detallado de todos los obstáculos que puedan interferir en el rango de la señal porque la atenuación que se presenta varia con el material (ver tabla 5). Estos pueden ser, paredes gruesas, puertas metálicas.

Material del obstáculo	Atenuación introducida
Madera	Baja
Plástico	Baja
Materiales sintéticos	Baja
Cristal	Baja
Cuerpo humano	Media
Ladrillos	Media
Mármol	Media
Agua	Media
Cerámica	Alta
Papel	Alta
Cemento	Alta
Cristal a prueba de balas	Alta
Metales	Muy alta

TABLA 5: Atenuaciones introducidas por obstáculos

Posibles focos de interferencias ya se había hecho mención sobre este aspecto cabe anotar otros factores como microondas, pantallas y otras redes cercanas.

Solapar ligeramente las zonas de cobertura, se debe permitir itinerancia las zonas con exceso de cobertura puede ser conflictivo, recordemos que dentro de la red (mismo SSID) las tarjetas seleccionan el AP que este emitiendo mayor potencia.

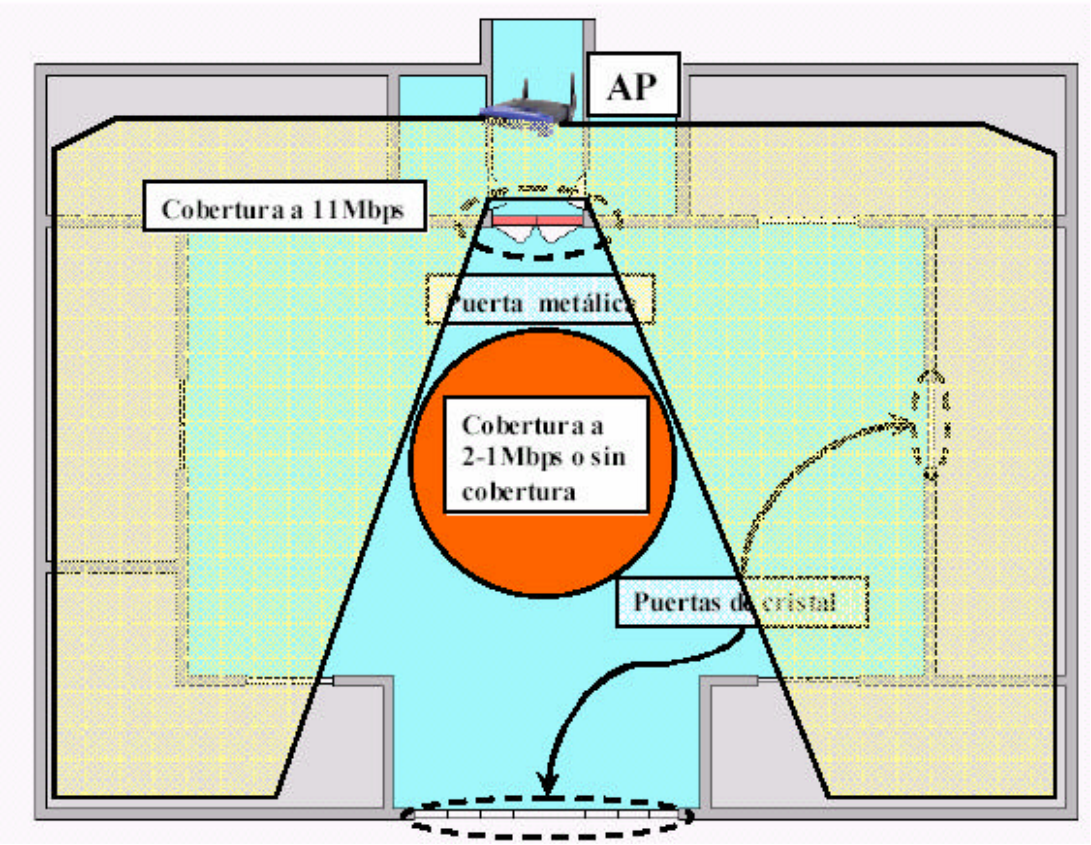

FIGURA 37: Cobertura de un punto de acceso con obstáculos

Una universidad de cinco plantas, con laboratorios en la planta baja. En la instalación ideal, en alguna parte de los laboratorios, debería haber un switch. El Switch será el centro de la infraestructura tanto cableada como inalámbrica.

En cada planta debería haber un Punto de Acceso inalámbrico que diese cobertura a esa planta. Si la planta tuviese una extensión importante, añadiríamos un segundo Punto de Acceso trabajando en modo repetidor.

Ahora se plantea el problema de cómo llevar la señal de red al punto de acceso de cada planta. Los Puntos de Acceso emiten una señal de red inalámbrica, pero esa señal de red les tiene que llegar vía cable (a menos que estén trabajando en modo repetidor). Existen formas de hacerles llegar la señal inalámbricamente pero complica, en muchas ocasiones de forma innecesaria, la instalación, entonces si se quiere hacer una configuración ideal el punto de acceso de cada planta deberá estar unido vía cable al switch

En muchos casos la planta es de gran superficie o tiene formas o estructuras que no permiten que la estructura basada en un punto de acceso y un repetidor sea suficiente. En esos casos, podemos añadir más repetidores, teniendo en cuenta que un repetidor no puede hacer de "repetidor de repetidor", es decir, un repetidor repetirá la señal de un PA pero no la de otro repetido, así que no podemos alargar

la cobertura indefinidamente con repetidores. De hecho, en la planta baja ya hemos puesto dos repetidores, podríamos hacer los mismos en las dos plantas superiores.

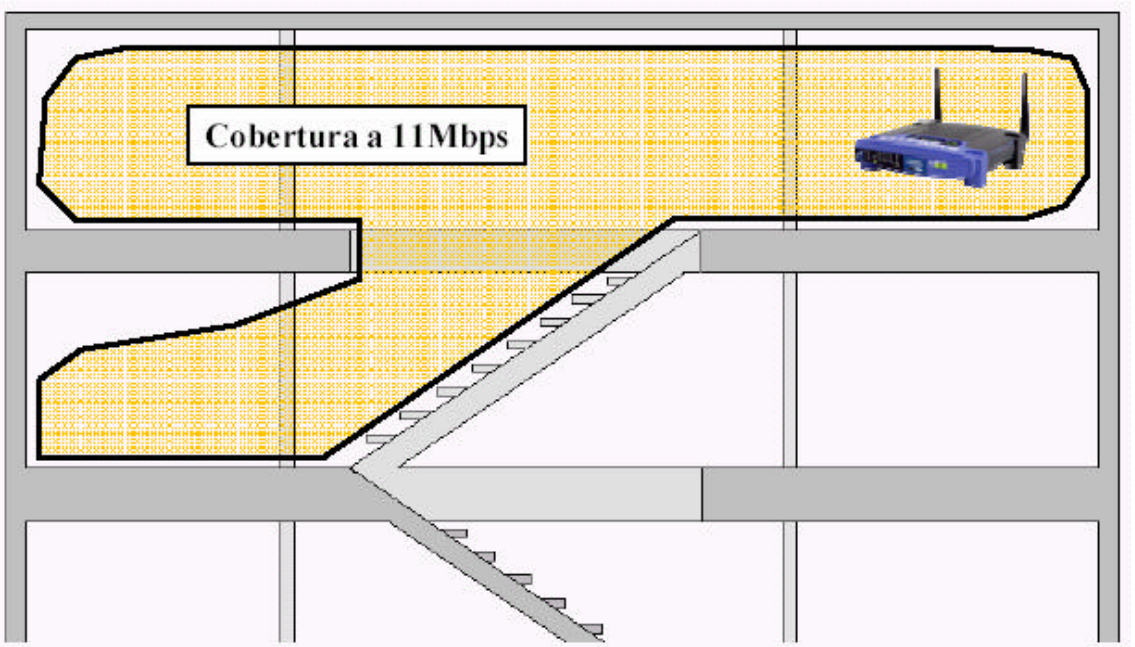

FIGURA 38: Cobertura de un punto de acceso en un posible piso

6.2.4 Selección y sintonización de canales.

1**.** Si es necesario convivir con otras redes que invadan nuestra área deseada de cobertura o necesitamos situar más de un punto de acceso dando cobertura en la misma zona se recomienda para estos casos.
Sintonizar los APs en canales suficientemente separados, puesto que la interferencia puede penalizar hasta en un 50% las restaciones.

2. cuando Situemos sobre el plano los APs y dibujemos sus zonas de cobertura, podremos seleccionar los canales en los que se sintonizaran los APs, para esto disponemos de los canales no solapados (1, 6, 11), y ubicaremos los canales lo más alejados posibles (separados, al menos, en 5 canales).

3. Si las celdas se solapan muy poco no es tan apremiante el problema de la interferencia.

4. Algunos fabricantes ofrecen software que facilita esta planificación, también hay paginas web (http://www.e-advento.com/tecnologia/calculos.php) que ofrecen el recurso de calculo para:

Análisis de un enlace wireless: Calcula aproximadamente los niveles de recepción y las perdidas en un enlace wireless.

Antena Isolation Calculador: Calculates isolation for horizontal & vertical antenas

Perdidas en zonas urbanas: Calcula aproximadamente las pérdidas en zona urbana entre dos antenas.

Perdidas en espacio libre: Calcula las pérdidas en espacio libre entre dos antenas.

Calculo de Ganancia y Punto Focal de una Antena Parabólica: Calcula la ganancia, el punto focal, y las distancias de la radiación para antenas parabólicas

Cálculo del radio de la zona Fresnel: Calcula el radio de la zona Fresnel entre dos antenas.

Cálculo de la inclinación de la antena Up/Down: Calcula la inclinación requerida de la antena para compensar para la curvatura de la tierra.

Calcula la Distancia y la Orientación: Calcula la distancia y la orientación entre dos puntos geográficos.

Análisis de la Amplitud de Rayo de una Antena Omnidireccional: Estima la cobertura de un patrón vertical de la antena.

Análisis de los factores Ambientales: Analiza factores ambientales a tener en cuenta.

Calculo de pérdidas Por Difracción: Cuando un obstáculo está ubicado entre el transmisor y el receptor sigue pasando un poco de energía gracias al fenómeno de difracción en el borde superior del obstáculo. Cuanto más alta la frecuencia de la transmisión más alta será la pérdida.

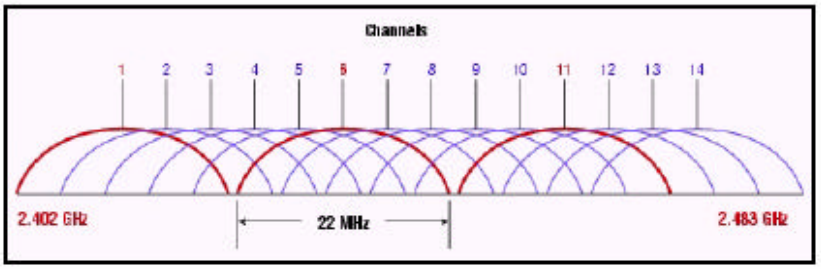

FIGURA 39: Canales de frecuencia

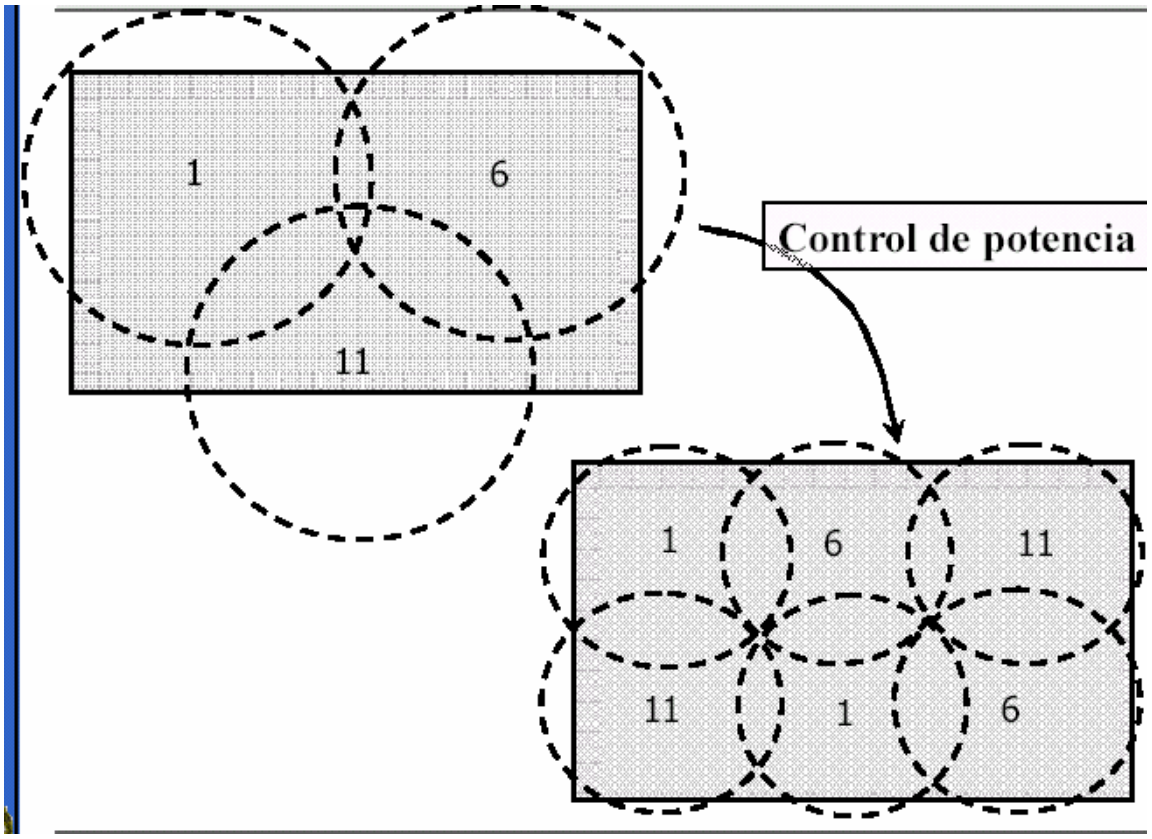

FIGURA 40: Control de potencia

6.2.5 Implantación de medidas de seguridad.

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

Aunque ya se explico el tema de seguridad a continuación se muestran algunas recomendaciones

1. Elegir un SSID que no identifique a nuestra red o al fabricante de nuestros equipos: Nunca dejar el SSID por defecto del fabricante, no dar pistas al atacante de la red de la que recibe cobertura.

2. Deshabilitar el broadcast del SSID: No anunciar nuestra red, si es posible.

3. Utilizar siempre Open Authentication: Deshabilitar la Shared Key Authentication.

4. Habilitar el filtrado de direcciones MAC: Si la finalidad de nuestra red nos los permite.

5. Algoritmos de encriptación: Habilitar como mínimo WEP, parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado

6. En entornos universitarios la opción más adecuada es implementar una solución WPA con servidor de autentificación RADIUS.

7. Cambiar de forma constantemente la clave: La opción más recomendable es actualizar el firmware/driver de los equipos y utilizar WPA-PSK.

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

Para la implementación de medidas de seguridad en WPA-PSK, se plantearan un ejemplo dando unos objetivos, se configuran un router de una marca aleatoria y se explicara el modo de funcionamiento.

Si se configura un Router inalámbrico LinkSys para permitir el acceso a clientes inalámbricos y cableados a Internet tendrá disposición de Servidor DHCP y NAT.

Se configura un PC para permitir la utilización del adaptador USB LinkSys

Se configura el protocolo WPA-PSK en ambos lados de la comunicación para garantizar la seguridad de las comunicaciones, aquí se utilizan los dos esquemas de codificación disponibles: TKIP, AES.

Se debe comprobar las prestaciones alcanzadas: el Servidor ftp en la nuestra red interna: con cliente cableado y cliente inalámbrico y el Servidor ftp en el exterior de la red interna: también con Cliente cableado y Cliente inalámbrico.

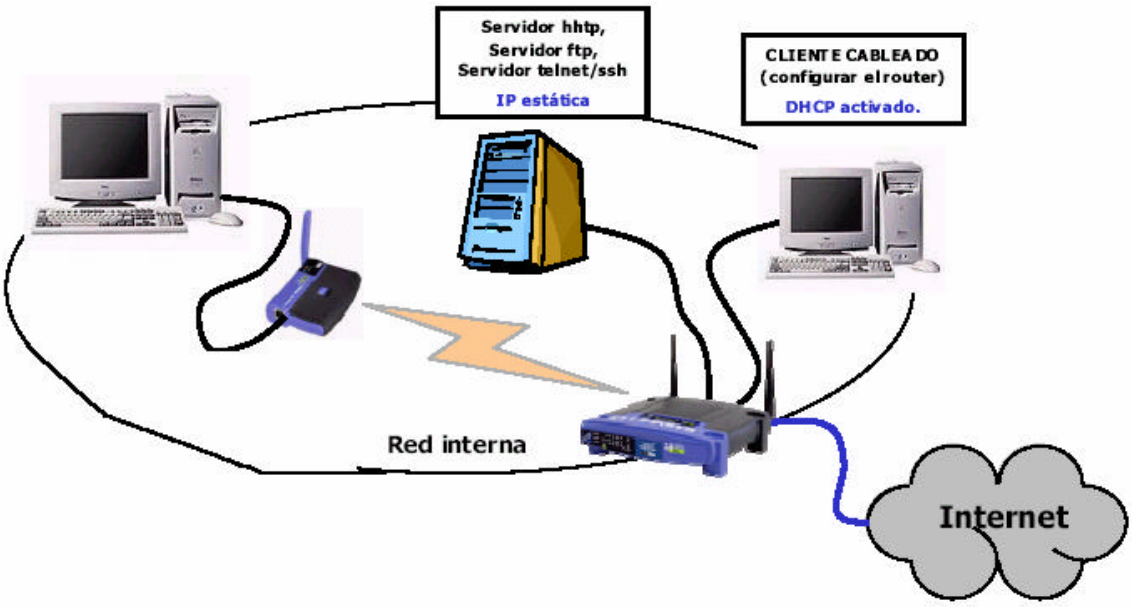

FIGURA 41: Escenario común

Configuración del cliente cableado:

Se darán unas direcciones aleatorias y otras vienen por defecto de fábrica

1. los equipos se utilizarán como el medio de acceder vía web a nuestro router y poder configurarlo. (también ver anexo 2)
Procedimiento de la configuración seria:
Ponchar mediante un cable Ethernet un equipo de sobremesa a una de las bocas que dan servicio a la zona cableada interna de nuestra red en el router inalámbrico.

Permitir que el equipo tome la dirección IP desde un servidor.

Realizar un petición http a la dirección ejemplo 192.168.1.1 IP por defecto en la interfaz privada del router inalámbrico.

FIGURA 42: Panel trasero del router

2. Introducir como password admin (password por defecto de router).

3. se debe cambiar la password a xxxxxxxxxxx (Administration -Management).

4. Asignarle parámetros IP estáticos a la interfaz pública (Setup - Basic Setup): IP, mascara, puerta de enlace, DNS1, DNS2 y DNS3

5. Deshabilitar el broadcast del SSID.

6.Activar al autentificación mediante WPA (Wireless - Wireless Security - Security Mode).

7. Seleccionar como método de encriptación TKIP o AES (Wireless -> Wireless Security - WPA Algorithms).

Con el software adecuado que en algunos casos traen los equipos, el administrador de la red podrá controlar los nodos locales y remotos desde un punto central o desde cualquier punto en la red. También controlara rápidamente las operaciones de la red puesto que estos softwar poseen interfase grafica dinámica.

También se pueden fijar parámetros de seguridad fijar el ancho de banda del RF y la frecuencia de operación.

6.3 MANTENIMIENTO DE LAS REDES

Como responsables del despliegue de la redes Wi-Fi se debe conocer que su mantenimiento puede ser una tarea muy ardua, con continuas caídas y degradaciones en el funcionamiento. Sin embargo esta tarea no tiene porque ser así, siendo equiparable al de una red cableada. Las razones de ello son múltiples:

la primera de ellas y principal factor es partir desde el primer momento con un diseño e implantación inicial de la red incorrecta, defectuosa o no adecuadamente dimensionado. A continuación le suele seguir un importante descuido en las labores de mantenimiento elementales, las cuales evitarían la mayoría de las incidencias posteriores, y no se implantan las herramientas necesarias para una adecuada gestión. El origen de todos estos descuidos u omisiones hay que buscarla en la muy escasa importancia que se le da a la implantación de una red inalámbrica. A continuación se analizará la problemática del mantenimiento.

Áreas de mantenimiento

Las principales son:

Entorno radio
Esta es un área que es exclusiva de entornos inalámbricos y que no existe en redes cableadas. Comprende los problemas que generan las interferencias entre celdas de la propia red o con otras redes, perturbaciones radioeléctricas de otros aparatos (hornos microondas, radares, móviles) y redes de otras tecnologías (bluetooth, telefonía inalámbrica doméstica, repetidores TV en el hogar). Al emplearse una parte del espectro radioeléctrico que no requiere de licencias específicas para su uso y que además es empleada de forma libre por multitud de tecnologías y aparatos domésticos, es un importante foco de conflictos.

En múltiples ocasiones la fuente de perturbaciones sólo emite potencia apreciable durante un breve periodo de tiempo (hornos de microondas, teléfonos inalámbricos), generando mal funcionamientos aleatorios que complican su identificación. En otras, la implantación de una nueva red con excesiva potencia en las cercanías y operando en la misma frecuencia o una muy próxima, fuerza a una replanificación de las frecuencias, tarea que puede ser compleja si se dispone de numerosos puntos de acceso. En otros casos existe una perturbación continua que aunque no llega a cortar las comunicaciones, degrada en mayor o menor medida las prestaciones (reducción en la velocidad binaria) y que puede ser laborioso de detectar para el responsable o usuario, o puede ser justificada erróneamente como exceso de tráfico o usuarios conectados.

Equipamiento
Puntos de acceso, antenas, cableado (coaxial, estructurado, eléctrico), networking, etc. requieren del normal cuidado. Nuevas actualizaciones de firmware o drivers deberán ser realizadas cuando el experto lo aconseje. En el caso de instalaciones exteriores, se debe tener en cuenta la aceleración de la degradación de los equipos por las inclemencias del tiempo y los casos de robos y vandalismo (también presentes en instalaciones públicas), lo cual suele afectar sobre todo a antenas, cableado y puntos de acceso.

Seguridad

Periódicamente es necesario cambiar las claves si son estáticas; las altas, bajas y modificaciones de usuarios deberán introducirse en el Radius; las direcciones MAC también tendrán que declararse; las aplicaciones deberán actualizarse para cerrar posibles agujeros de seguridad; analizar posibles intrusiones; etc. Aunque estas tareas parecen de un mayor volumen que para el caso de redes fijas, si estas últimas están adecuadamente sectorizadas, entonces el mantenimiento es análogo.

Gestión de uso

Tráfico circulante, número de usuarios, velocidades binarias alcanzadas, distribución del uso entre celdas.

ANEXOS