UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS
VERITATE SOLA NOBIS IMPONETUR VIRILISTOGA. 1948

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

"Diseño de red inalámbrica en el Centro de Convenciones Bolívar"

Tesis presentada en opción al título estatal de

Master en Ciencias

Autor: Ing. Luis Enrique Hernández Lugones

Tutor: Mcs. David Beltrán Casanova

Santa Clara, Cuba

2010

"Año 52 de la Revolución"

Universidad Central "Marta Abreu" de Las Villas
Facultad de Ingeniería Eléctrica
Departamento de Telecomunicaciones y Electrónica

"Diseño de red inalámbrica en el Centro de Convenciones Bolívar"

Autor: Ing. Luis Enrique Hernández Lugones

Tutor: MSc. David Beltrán Casanova
Prof. Dpto. de Telecomunicaciones y Electrónica
Facultad de Ing. Eléctrica. UCLV.
e-mail: beltran@uclv.edu.cu

Santa Clara

2010

"Año 52 de la Revolución"

Hago constar que el presente trabajo en Opción al Titulo Estatal de Master en Ciencias fue realizado en la Universidad Central “Marta Abreu” de Las Villas como parte de la culminación de estudios de Maestría en Telemática, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

TAREAS TÉCNICAS

Las tareas a realizar en este trabajo son:

- Revisión y estudio bibliográfico sobre la actualidad de las redes inalámbricas en el mundo.
- Visitar instituciones donde existen redes inalámbricas, como variantes de estudio.
- Definir y especificar el tipo de tecnología a usar para lograr eficiencia en el enlace.
- Confección del proyecto para enlazar las áreas del proyecto.

Firma del Autor

Firma del Tutor

Agradecimientos

A mis profesores de la maestría

A mi tutor David Beltrán Casanova

A mis compañeros de trabajo

A toda mi familia

Dedicatoria

A mis padres

A mi esposa

A mi hija

Resumen

RESUMEN

Se realizó el estudio para el diseño de una red inalámbrica de área local, con el objetivo de enlazar áreas que están fuera de una red, para dar solución a los problemas de interconexión en lugares de difícil instalación de una infraestructura cableada. El objeto de aplicación de los resultados de esta tesis lo constituye el enlace inalámbrico entre estas áreas y la red cableada del Centro de Convenciones Bolívar, logrando de esta forma adicionar a la red de computadoras de este centro todas las áreas del mismo. Se tuvo en cuenta para el diseño la distancia entre los puntos a enlazar, la altura y ubicación a la que deben estar las antenas y puntos de acceso, de forma tal que no se vea afectada la zona libre de Fresnel. Se definió todo el equipamiento necesario y se hizo el diseño del radio enlace para el mismo de forma tal que cumpliera los requisitos técnicos normados.

Para la realización de este trabajo se revisaron diversas fuentes bibliográficas y se realizó un estudio de las áreas a cubrir con los enlaces teniendo en cuenta las distancias de cobertura del enlace, las características de los materiales constructivos de las edificaciones, las condiciones del entorno, la seguridad en esta subred, la cantidad de usuarios a servir, accesibilidad y la autenticación de los mismos. Luego con los resultados del estudio y el análisis de los diferentes estándares de la norma 802.11 de la IEEE se propone el equipamiento adecuado para el montaje de una red inalámbrica capaz de solucionar la cobertura total de todas las áreas del Centro de Convenciones Bolívar.

Índice

INDICE

Introducción

INTRODUCCIÓN

Las comunicaciones vía radio, han experimentado un gran auge en nuestros días, debido a los cambios constantes en las características físicas y funcionales de los equipos utilizados para este tipo de comunicación. Las redes inalámbricas usan el aire como medio de transmisión y se han convertido en una variante muy necesaria para unir lugares donde es imposible llegar con redes cableadas. Al igual que las redes con cables LAN, WAN, MAN, existen redes inalámbricas WLAN *(WLAN, Wireless Local Area Networks)*, WPAN, WWAN/WMAN. Ejemplo de estas redes lo constituyen los estándares IEEE 802.11, Bluetooht (802.15.1), Home RF, HiperLan, MobileFi (802.20), WiMax (802.16), ZigBee (soportada sobre la base de 802.15.4), entre otros. El origen de las Redes de Área Local Inalámbricas data de 1979, cuando el Instituto de Ingenieros Eléctricos y Electrónicos (*IEEE, Institute of Electrical and Electronic Engineer*) publicó los resultados de un experimento realizado por ingenieros de la IBM (*International Business Machine*) en Suiza. En mayo de 1985 la *Comisión Federal de Comunicaciones (FCC, Federal Communications Comission*), asignó las bandas *Médicas, Científicas e Industriales (ISM, Industrial, Scientific and Medical)*. En 1990 se forma el comité IEEE 802.11, con la tarea de generar normas para las WLAN y no es hasta el año 1997 que se ratifica la especificación 802.11 original como la norma para las WLAN. Los países punteros en redes WLAN son los Estados Unidos, países miembros de la Unión Europea, Australia y Japón, todos del mundo desarrollado. Cuba, como otros tantos países en vías de desarrollo, ha asumido el reto de las redes WLAN; y ya varias empresas e instituciones se han sumado al empleo de las mismas. En la zona central del país podemos citar como

algunos ejemplos la OBE, Hoteles de la Cayería Norte de Villa Clara, Radio Cuba, Etecsa, Copextel, Movitel, Cubalse, Sepsa, ECIE, Universidad Central “Marta Abreu” de la Villas y con este trabajo pretendemos introducir este nuevo tipo de tecnología para dar cobertura a la totalidad del campus del Centro de convenciones Bolívar.

Este trabajo surge porque existen áreas del centro de Convenciones Bolívar que no se pueden unir a la estructura central de la red, debido a lo difícil y costoso que resultaría instalar una red cableada en las áreas que se quieren enlazar, principalmente en salones de reuniones con capacidad superior a 100 usuarios, además de otras áreas que por las características de esta institución necesitarían contar con enlace permanente para que los usuarios puedan hacer uso de la movilidad sin perder el enlace, actualmente dichos locales están privados de todos los servicios que brinda la red CCB, constituye esto sin dudas un problema técnico al estar alejados de todo el proceso de informatización en que esta inmerso el país.

Con el diseño que propone este trabajo se logrará enlazar de manera inalámbrica a la red CCB todo el campus del Centro de Convenciones que hoy esta fuera del alcance de los servicios que presta la red. La solución a los anteriores problemas contribuirá a elevar el desarrollo tecnológico y la consiguiente calidad en los servicios al cliente, y constituye claramente un objetivo de desarrollo de este trabajo. Los resultados alcanzados pueden ser de conocimiento de todos los interesados en el tema, constituyendo una metodología que sirve de guía para trabajos futuros en este aspecto de las Telecomunicaciones.

Objetivo general:

Dimensionar la red inalámbrica para el Campus del Centro de Convenciones Bolívar, teniendo en cuenta accesibilidad, autenticación y seguridad de redes.

Objetivos específicos:

- Realizar estudio sobre la definición de redes inalámbricas y sus diferentes estándares y principales características.
- Concepción del diseño teórico de un enlace inalámbrico.
- Estudiar el equipamiento que se comercializa en el mundo en soluciones inalámbricas y obtener definiciones y características técnicas, según las condiciones cubanas y cumpliendo los requerimientos técnicos para su instalación, que proporcionen un enlace estable y con tasas de transferencia de datos aceptables.

Entre los principales resultados alcanzados en este trabajo se tienen:

- Lograr incluir a través de enlaces inalámbricos áreas del Centro de Convenciones que están fuera de la Red CCB.
- Un procedimiento para el dimensionamiento, proyección, montaje y puesta en marcha de redes y subredes inalámbricas en el Centro de Convenciones Bolívar.
- Un procedimiento para la accesibilidad y autenticación de usuarios, así como la implementación de la seguridad para este tipo de redes.
- Proyecto de subred inalámbrica conectando áreas del centro.

Capítulo I

CAPITULO I. LAS REDES WLAN

Las Redes Inalámbricas de Área Local, conocidas por sus siglas WLAN o Wi-Fi[1], son un sistema de transmisión de datos, que utiliza como medio de propagación el aire. Dicho sistema fue implementado como una extensión o alternativa de una red LAN cableada dentro de un edificio o de un espacio abierto.

Sin embargo, el costo y complejidad asociado a la infraestructura telefónica y el cableado tradicional para brindar acceso en áreas alejadas, creó un vacío significativo en la cobertura alrededor del mundo; limitando el acceso a las grandes ciudades y a sectores con los recursos económicos para implementar redes cableadas.

Estas limitaciones en las redes cableadas dieron paso a la introducción de soluciones inalámbricas al problema. Las redes de acceso inalámbricas no eran del todo desconocidas, ya en 1979 un grupo de ingenieros de IBM habían publicado los resultados de un experimento en Suiza, donde se utilizaban enlaces infrarrojos para crear una red local en una fábrica de ese país, el problema estaba en crear una red capaz de soportar las exigencias de los servicios. Con vista a lograr este objetivo la IEEE (*Institute of Electrical and Electronic Engineers*) ha creado desde el comienzo de los años 90' grupos de trabajo para la creación de estándares capaces de determinar las características y el funcionamiento de las redes de acceso inalámbricas [1].

[1] Wireless Fidelity es el nombre comercial que reciben las redes WLAN del estándar IEEE 802.11.

En la actualidad una red de acceso inalámbrica es una tecnología innovadora que presenta una serie de ventajas sobre las redes cableadas [2]:

- Movilidad
- Simplicidad
- Rapidez y flexibilidad en la instalación
- Costos de propiedad reducidos
- Escalabilidad

Estas ventajas la hacen una alternativa viable para dar solución a problemas relacionados con la implementación de redes para la transmisión y recepción de datos.

Por otro lado, la seguridad ha resultado ser una de las principales limitaciones frente a las redes cableadas , por la naturaleza propia del medio de transmisión que no reconoce fronteras, aunque ya se han creado protocolos de seguridad que la hacen más fuerte frente a penetraciones externas [3].

La siguiente figura muestra las diversas clasificaciones de las redes inalámbricas referidas a su ámbito de utilización.

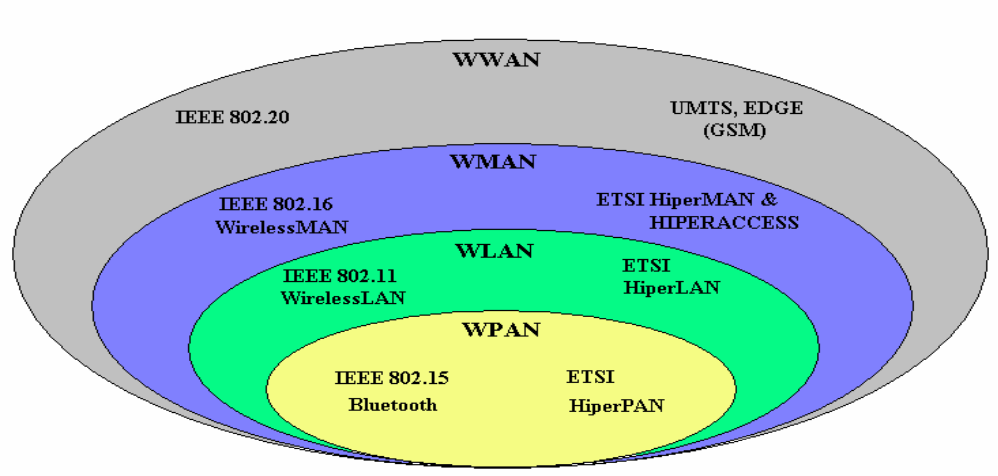


Figura 1.1: Clasificaciones de las redes inalámbricas.

Por supuesto estas redes de nuevo tipo no van a sustituir ni a eliminar las redes cableadas, de hecho la tendencia actual en las telecomunicaciones es la convergencia de tecnologías y estándares, por los que las redes de acceso inalámbricas solo serían un complemento o alternativa que permitiría la creación de redes aún más potentes [4].

1.1 Fundamentos de las WLAN

Estas son redes de acceso inalámbricas en las que dos o más terminales se comunican, sin la necesidad de utilizar cables, a velocidades de transferencias superiores a 1 Mbps [2]. En una WLAN se alcanza una cobertura cercana a los 100 metros lo que la hace ideal para entornos de oficina, aeropuertos, instituciones educativas y residencias familiares [5].

Este tipo de redes basa su implementación en un grupo de normativas donde se especifica una interfaz sobre el aire entre el cliente y la estación base o entre dos clientes inalámbricos mediante la definición del uso de los dos niveles más bajos de modelo de referencia OSI (*Open System Interface*): la capa física y la capa de enlace de datos [6].

En la capa física se define como realizar la transmisión y recepción de señales inalámbricas sobre un canal de RF (*Radio Frequency*) mientras que en la capa de enlace de datos se especifican mecanismos encargados del acceso al medio, la sincronización de tramas y control de potencia [1].

El estándar 802.11 o Wi-Fi (*Wireless Fidelity*) es la familia de especificaciones desarrolladas por la IEEE para WLAN [8]. En ella se hace uso de las bandas ISM (*Industrial, Science and Medical*) de 2.4 GHz y 5 GHz, bandas reservadas para el uso no comercial del espectro de frecuencia cuyo uso está abierto a todo el mundo sin necesidad de licencia, siempre y cuando se respeten los niveles de potencia trasmitida [7].

Tecnologías en WLAN

La utilización de ondas electromagnéticas para trasmitir información de un punto a otro sin la existencia de conexiones físicas ha otorgado a las WLAN varias posibilidades para lograr su objetivo. Una de ellas es el uso de ondas infrarrojas aunque con esta se limita el uso de las WLAN a cortas distancias donde haya línea de vista; la otra posibilidad recae en el uso de ondas de RF. En esta última sobresalen técnicas de modulación como la técnica de espectro extendido y la técnica de banda estrecha [3].

La técnica de espectro ensanchado o extendido consiste en difundir la señal de información a lo largo del ancho de banda disponible. Las dos variantes de esta técnica son: FHSS (*Frequency Hopping Spread Spectrum*) y DSSS (*Direct Sequence Spread Spectrum*) [8].

FHSS consiste en trasmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo inferior a los 400 ms, transcurrido ese tiempo se cambia a otra frecuencia de acuerdo a una secuencia de *spreading*. De esta manera cada sección de información se va transmitiendo en una frecuencia diferente durante un intervalo muy corto de tiempo. Esto posibilita que múltiples sistemas puedan coexistir en la misma área mientras usen diferentes secuencias de *spreading*, otorga alta seguridad y permite más de tres enlaces. Sin embargo esta técnica no permite altas velocidades y causa retraso debido a que su señal es angosta y que en el proceso de comunicación la señal tiene que parar y resincronizar [6].

Con DSSS el flujo de bits de entrada se multiplica por una señal de una frecuencia mayor, basada en una función de propagación determinada. Esta señal de entrada concentrada se dispersa a varias frecuencias ocupando todo el canal, disminuyendo así la potencia de transmisión [3]. Con el ancho de banda extra se hacen varias copias de la señal original por lo que si la interferencia presente en el canal no afecta a todas las frecuencias entonces los datos se pueden recuperar sin pérdida alguna. DSSS garantiza tres canales para tres enlaces, cada canal con

22 MHz de ancho de banda, lo que permite alcanzar altas velocidades de transferencia de datos [6].

En la técnica de banda estrecha se emplea OFDM (*Orthogonal Frequency Division Multiplexing*). Actualmente esta técnica reviste gran importancia en las redes de acceso inalámbricas debido a las facilidades que otorga. Las características de esta tecnología y su funcionamiento serán tratadas en capítulos posteriores de este trabajo.

IEEE 802.11

El estándar original de esta familia se publicó en julio de el año 1997 y especifica velocidades de datos de 1 y 2 Mbps que se trasmiten por señales infrarrojas o utilizando la banda ISM a 2.4 GHz. Esta norma define el protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) como método de acceso y emplea como técnicas de utilización del medio radioeléctrico, FHSS (*Frequency-hopping spread spectrum*) y DSSS (*Direct-sequence spread spectrum*) [1].

Cada vez que se percibe la necesidad de implementar nuevas técnicas para resolver un determinado problema asociado a las WLAN, la IEEE crea un nuevo grupo de trabajo incluido en el estándar 802.11 e identificado por una letra. La solución al problema queda plasmada en una nueva especificación que se identifica por la misma letra que su grupo de trabajo. Hoy en día las especificaciones más populares corresponden a la letra *a*, *b* y *g* [6].

IEEE 802.11b

La primera modificación realizada al estándar original apareció en 1999 y fue designada como IEEE 802.11b. En ella se permiten una tasa de transmisión de 1, 2, 5.5 y 11 Mbps de acuerdo a la distancia entre el usuario y el punto de acceso. En el se utiliza la banda de los 2.4 GHz y se ratifica CDMA/CA como método de acceso al medio [7].

Los primeros equipos basados en esta norma aparecieron rápidamente ya que como técnica de modulación utilizaba una extensión a la modulación DSSS del estándar original. El aumento de la velocidad, el reducido costo de

implementación, así como la compatibilidad entre los productos de diferentes proveedores permitieron un crecimiento de usuarios de esta tecnología. Otra facilidad que entrega este estándar es que si al estar trasmitiendo a 11 Mbps la calidad del enlace se empobrece es posible trasmitir a 5.5, 2 y 1 Mbps ya que en estos se utilizan métodos más redundantes de codificación de datos [6].

Esta especificación divide el espectro en 14 canales solapados de 22 MHz de ancho de banda, a una distancia de 5 MHz cada uno. La canalización para este tipo de redes se realiza de acuerdo al país donde se utilice. En Estado Unidos se utilizan 11 canales dando lugar a un grupo de tres canales no solapados (Figura 1.2), en Europa 13 canales con tres grupos de tres canales no solapados y Japón que emplea los 14 teniendo cuatro grupos de tres canales no solapados. Este tipo de canalización requiere importancia vital a la hora de configurar la red ya que utilizar los grupos de canales no solapados permite evitar interferencias en celdas adyacentes [2].

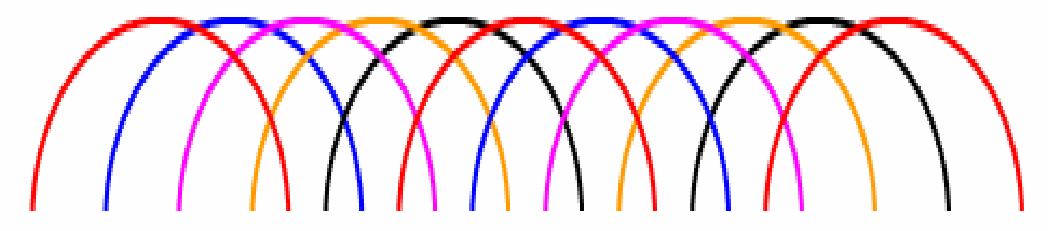


Figura 1.2: Canalización DSSS en USA. Un grupo de tres canales no solapados, el 1, el 6 y el 11.

IEEE 802.11a

En el mismo año 1999 se publica también la revisión 802.11a del estándar original pero no es hasta el 2001 que empiezan a aparecer los primeros equipos basados en esta especificación, empezándose a utilizar en Estados Unidos y Japón con clara desventaja respecto a su predecesor, el estándar 802.11b, mientras que en Europa no fue admitido hasta el 2003 [6].

Este estándar alcanza velocidades de transmisión de hasta 54 Mbps muy superiores a los 11 Mbps de su predecesor y opera a 5 GHz lo que le otorga una

menor probabilidad de interferencia aunque condiciona las instalaciones a disponer de línea de vista y disminuye su alcance debido a que sus ondas se absorben fácilmente. Por último se utiliza la técnica OFDM sobre ocho canales no solapados lo que aseguraría ocho puntos de acceso no interferentes entre ellos permitiendo un mayor porcentaje de usuarios, aspecto importante a la hora del diseño de redes principalmente en la escalabilidad de las mismas [5].

Sin embargo, no son las limitaciones asociadas al uso de la banda de 5 GHz ni insertarse tarde en el mercado inalámbrico la causa principal de la poca popularidad de esta especificación. La principal deficiencia y causa principal de la poca popularidad de 802.11a radica en su falta de compatibilidad con el estándar 802.11b. En buscas a solucionar esta deficiencia comenzaron a aparecer equipos bimodos que permiten el uso de la banda de 2.4 GHz y 5 GHz en una misma WLAN [8].

IEEE 802.11g

En el año 2001 es aprobada por la IEEE una nueva especificación para redes de área local inalámbricas, el estándar 802.11g. Presentado como la evolución de la norma 802.11b utiliza la banda de frecuencia de 2.4 GHz y mantiene el uso de DSSS como técnica de modulación, sin embargo lo novedoso se encuentra en incorporar la técnica OFDM. La inclusión de OFDM condicionó que este estándar alcanzara altas velocidades de transmisión de hasta 54 Mbps, similar a la del estándar 802.11a [1].

Otro aspecto importante es que permite la interoperatividad con la norma 802.11b, limitándose a utilizar 3 canales sin solapamiento de igual ancho de banda. Sin embargo, en redes bajo el estándar g la presencia de estaciones bajo la norma b reduce significativamente la velocidad de transmisión [8].

Desde hace algunos años algunas compañías han adicionado una característica adicional o protocolo propietario a sus equipos permitiendo que redes diseñadas bajo 802.11g dupliquen sus velocidades de transmisión. A pesar de aumentar las velocidades de la red, el ser protocolo propietario y no una solución generalizada,

ocasiona conflictos con otros equipos provocando que en muchos casos no sea compatible con redes inalámbricas actuales [6].

IEEE 802.11n

En septiembre del año 2009 se hace oficial la norma que hasta este momento se nombraba *Draft 2.0* que desarrolla una nueva especificación que permite aumentar las velocidades de transferencia de datos superiores a los 100 Mbps [5].

Presentada como la evolución de la norma 802.11g utiliza la banda de frecuencia de 2.4 GHz y 5 GHz mantiene el uso de OFDM como técnica de modulación, sin embargo lo novedoso se encuentra en incorporar la técnica MIMO. La inclusión de MIMO condicionó que este estándar alcanzara altas velocidades de transmisión de hasta 600 Mbps, muy superior a los anteriores estándares de la IEEE 802.11.

Otro aspecto importante es que permite la interoperatividad con las normas 802.11a y 802.11g, lo cual significa un gran sacrificio de recursos técnicos ya que los entornos que limitan el ancho del canal a 20MHz serán sobrecargados con los costos adicionales de implementaciones MIMO complejas a fin de lograr el rendimiento requerido [9].

Fundamentación teórica de las tecnologías empleadas en el estándar IEEE 802.11n.

La principal característica que define lo esperado en las nuevas generaciones de WLAN es el incremento de la velocidad de transmisión. Teniendo en cuenta que no va a ser posible aumentar la potencia de emisión por encima de los valores actuales, las investigaciones para elevar la velocidad de transmisión se han centrado en desarrollar nuevos sistemas de modulación, detección y antenas que permitan transmitir y recibir regímenes binarios más altos y con mayor eficiencia [2].

Sin embargo, mejorar la interfaz de radio requiere tener en cuenta una característica intrínseca de las comunicaciones de radio en enlaces terrestres, la propagación multitrayecto. Este fenómeno se puede resumir diciendo que al receptor llegan varias réplicas de la señal con diferentes retardos entre ellas a

causa de difracciones y reflexiones por obstáculos que encuentra la señal en su trayectoria (Figura 1.3). Esto ocasiona una drástica reducción del nivel de la señal en el receptor como resultado de una combinación “destructiva” de señales con trayectorias diferentes [4].

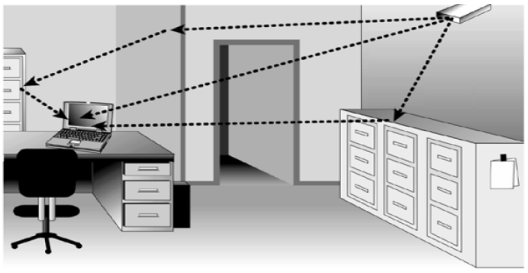


Figura 1.3: Efecto multitrayecto.

Con vistas a enfrentar estos retos el grupo encargado de desarrollar la especificación 802.11n se apoyó en dos tecnologías fundamentals, OFDM (*Orthogonal Frequency Division Multiplexing*) y MIMO (*Multiple Input Multiple Output*) [9]:

1.1.1 OFDM

Es una técnica de modulación que utiliza múltiples portadoras ortogonales, cada una modulada en amplitud y fase para la transmisión de datos [3]. Aunque esta tecnología fue presentada hace más de 30 años, no es hasta finales de la década de 1980 que los avances tecnológicos hicieron factible su implementación [8].

Con la aparición de las redes inalámbricas, OFDM se convirtió en una tecnología prometedora ya que permite lograr altas razones de datos e incrementa la robustez de las comunicaciones inalámbricas frente al desvanecimiento causado por el multitrayecto [8].

La misma hace uso de dos herramientas esenciales, la modulación de múltiples portadoras y el principio de ortogonalidad [6].

La técnica de modulación de múltiples portadoras divide un flujo de alta tasa de transferencia de datos en varios flujos paralelos de tasas de transferencia

menores para después modular cada uno en una subportadora. Un sistema de datos paralelos clásico divide la banda de frecuencia de la señal en N subportadoras no solapadas, donde cada subportadora es modulada y multiplexada en frecuencia. El uso de subportadoras no solapadas logra evitar la interferencia entre estas pero conlleva a un uso ineficiente del espectro [7].

Para eliminar esta ineficiencia OFDM propuso el uso del criterio de ortogonalidad entre las subportadoras. Haciendo uso de ese criterio se implementó un sistema de datos paralelos multiplexados en frecuencia utilizando subportadoras solapadas, donde la ortogonalidad evitaría que las subportadoras se interfirieran entre ellas [6].

La Figura 1.4 muestra la diferencia entre la técnica de múltiples portadoras sin solapamiento y la técnica de múltiples portadoras utilizando solapamiento. Como se puede apreciar con esta última se puede salvar cerca del 50% del ancho de banda.

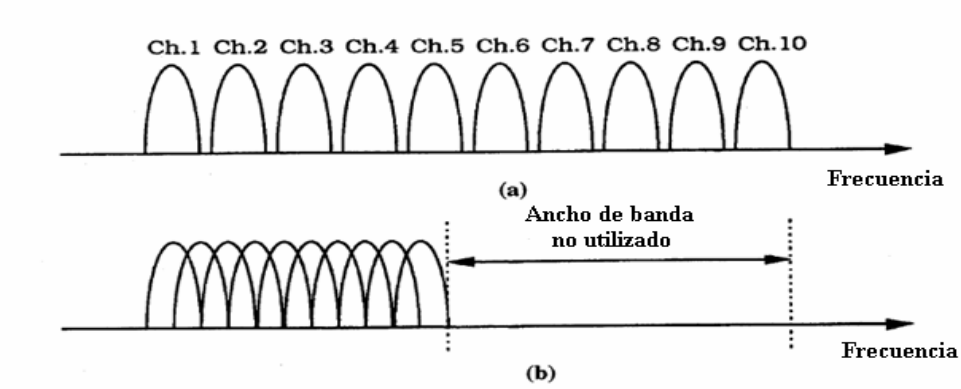


Figura 1.4: Técnicas de múltiples portadoras.

(a) Técnica de múltiples portadoras convencional.

(b) Técnica de modulación ortogonal con múltiples portadoras.

En cuanto a la modulación de las subportadoras en un múltiplex OFDM, cada una de ellas se modula con una información diferente, aunque por facilidad de implementación, el sistema de modulación suele ser el mismo para todas ellas, como QPSK (*Quaternary Phase Shift Keying*) o n2-QAM (*Quadrature Amplitude*

Modulation). Además se suelen reservar algunas portadoras para transmitir información de sincronismo y ecualización espectral o bien para establecer canales de servicios [8].

1.1.2 OFDM vs interferencia multitrayecto: intervalo de guarda y extensión cíclica

OFDM implementó un mecanismo con vista a casi eliminar los efectos de la interferencia por propagación multitrayecto. Este consiste en introducir un intervalo de guarda extendido cíclicamente para cada símbolo OFDM. Este tiempo de guarda es elegido superior a la mayor dispersión de retardo esperada para que las componentes multitrayecto de un símbolo no interfieran con el siguiente símbolo, mientras que la extensión cíclica evita la interferencia entre subportadoras [8].

1.1.3 OFDM en el estándar IEEE 802.11n

En el borrador de la especificación 802.11n, el primer requerimiento señalado por el grupo de trabajo era que este estándar soportara una implementación de OFDM que mejorara al 802.11a/g, usando una tasa de código más alta y escasamente más ancho de banda, mejorando las velocidades alcanzables a 65 Mbps de 54 Mbps de los estándares ya existentes [6].

Así 802.11n aumentó a 52 el número de subportadoras de datos de las 48 existentes en el estándar 802.11g y eliminó la redundancia presente en otras especificaciones utilizando una razón de código de 5/6. Además se introdujo una opción para reducir el intervalo de guarda a 400ns de los 800ns utilizados en especificaciones previas, incrementando la velocidad hasta 72Mbps [10].

Realizando el mismo análisis que en el epígrafe anterior, para un intervalo de guarda de 800 ns, la duración del símbolo en 802.11n se elige 5 veces superior:

$$5 \cdot 800\ \eta s = 4\,\mu s$$

Donde espaciamiento entre subportadoras es de:

$$4 - 0.8 = 3.2\ \mu s \qquad {}^{1}\!/_{3.2\ \mu s} = 312.5\ KHz$$

Con una razón máxima de transferencia de 65Mbps la cantidad de bits transmitidos en un segundo es:

$$65\ Mbps \cdot 4\ \mu s = 260$$

Para lograr esos 65Mbps se emplea la modulación 64-QAM y una razón de código de 5/6, permitiendo la transmisión de 5 bits por símbolo por subportadora. Con este valor se obtienen las 52 subportadoras de datos.

$$260\ {}^{}\!/_{5} = 52$$

Con 52 subportadoras de datos se puede hacer el cálculo de ancho de banda que ocupa la señal:

$$52 \cdot 312.5\,KHz = 16.25\ MHz$$

Lo que satisface la condición de 20 MHz de ancho de banda del canal.

1.1.4 MIMO

El uso de múltiples antenas tanto en el receptor como en el transmisor, sistema de antenas MIMO (Figura 1.5), es una tecnología emergente que permite la implementación de redes inalámbricas confiables y de altas razones de datos [11]. En un sistema MIMO cada equipo transmisor tiene asociado un número de antenas N, y cada receptor otro, igual o diferente al del transmisor, denotado como M. Desde el punto de vista de la propagación, el canal de radio no es único ya que existe un canal entre cada antena transmisora y cada antena receptora, lo que obliga a representar la propagación mediante una matriz H (N•M). En esta matriz el elemento hij representa la función de transferencia compleja entre la antena transmisora j y la antena receptora i [2].

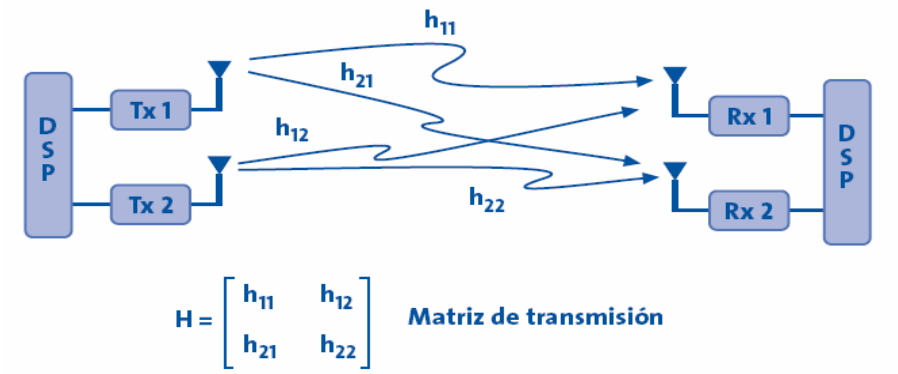


Figura 1.5: Esquema MIMO de 2x2 antenas.

Generalmente la señal multitrayecto es considerada como interferencia, reduciendo la capacidad de recuperar la información en el receptor, sin embargo MIMO utiliza en su beneficio este fenómeno para mejorar la calidad y capacidad del enlace [12]. De forma más específica, esta mejora del enlace viene dada por la ganancia del arreglo de antenas, la ganancia por diversidad, la ganancia por multiplexación y cancelación de interferencia [13].

En general hay dos categorías importantes en los sistemas MIMO:

De lazo abierto: Donde el transmisor no tiene la información del estado del canal y envía los datos directamente hacia el receptor sin recibir ningún tipo de información por parte de este [13]. Esta categoría es capaz de manejar comunicaciones con receptores en movimiento y mantener la simplicidad en los circuitos pero es poco eficiente en el uso de los recursos del enlace [9].

De lazo cerrado: El transmisor conoce de forma completa o parcial la información del estado del canal con vista a adaptar la transmisión para mejorar el comportamiento del enlace [13]. Conocer esta información se logra mediante el envío por parte del transmisor de señales de “entrenamiento” al receptor quien la recibe y analiza. Luego la información sobre la ruta es enviada al transmisor que selecciona la potencia y el esquema adecuado que mejor se acomode a esa ruta. Esta categoría mejora la eficiencia de los recursos del enlace, pero hace más complejo los circuitos necesarios para su implementación [9].

1.1.5 Multiplexación espacial

Uno de los grandes atractivos de la tecnología MIMO es ofrecer un incremento en la capacidad del enlace sin incrementar la potencia de transmisión o el ancho de banda, solo aumentando el número de antenas [4].

El principio que opera detrás de este aumento de capacidad se denomina multiplexación espacial y se basa en la utilización del concepto de división espacial. Si las diferentes trayectorias multitrayecto están suficientemente decorrelacionada, con N antenas en el transmisor y N en el receptor se pueden establecer N canales de comunicación independientes. La aplicación del mismo solo requiere que exista un adecuado espaciamiento entres las antenas tanto transmisoras como receptoras [2].

Utilizando este tipo de multiplexación, un sistema MIMO puede trasmitir y recibir flujos de datos paralelos e independientes a través de las múltiples antenas ubicadas en ambos terminales (Figura 1.6), incrementándose la razón de datos y la eficiencia espectral del enlace [5].

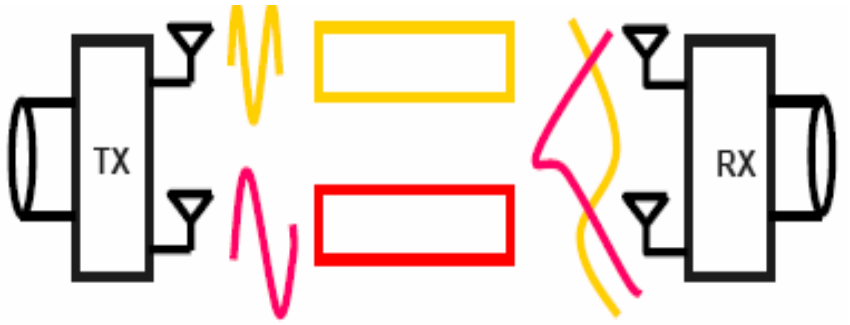


Figura 1.6: Multiplexación espacial en un sistema MIMO.

1.1.6 MIMO en IEEE 802.11n

El uso de MIMO en la especificación 802.11n permite al sistema aumentar la velocidad de transmisión linealmente con cada antena extra en ambos terminales, el receptor y el transmisor, gracias al efecto de la multiplexación espacial. El número máximo de antenas para este estándar es de 4 antenas en ambos

extremos del sistema, lo que permite alcanzar velocidades cercanas a 300Mbps [9].

IEEE 802.11n también incorpora un modo opcional que utiliza canales de 40MHz el doble de las especificaciones precedentes. Este crecimiento en ancho de banda, permite el doble de la capacidad alcanzada para canales típicos de 20MHz [10]. Así, con este modo opcional, se puede alcanzar una capacidad en el canal de 600Mbps.

Después de una descripción de OFDM y MIMO, tecnologías que mejoran la interfaz física del estándar 802.11n, se hace necesario examinar aquellas modificaciones introducidas en la capa MAC.

Uno de los objetivos de la creación de la especificación 802.11n es la obtención de velocidades superiores a 100Mbps en el MAC SAP (*Service Access Point*), para esto hace falta mejorar la eficiencia en la transferencia de datos. En estándares anteriores como 802.11a/g se alcanzaban velocidades de hasta 54Mbps en la capa física sin embargo se obtenían 24,7Mbps en la capa MAC SAP, lo que significa que el 45% del tráfico de información está asociado al encabezamiento de la trama [9].

Para lograr un mejor rendimiento, en este nuevo estándar, se emplea la utilización de secuencias de intercambio agregadas. Esto permite que varios paquetes de datos puedan ser transmitido utilizando solamente una sola cabecera. (Figura 1.7) [10].

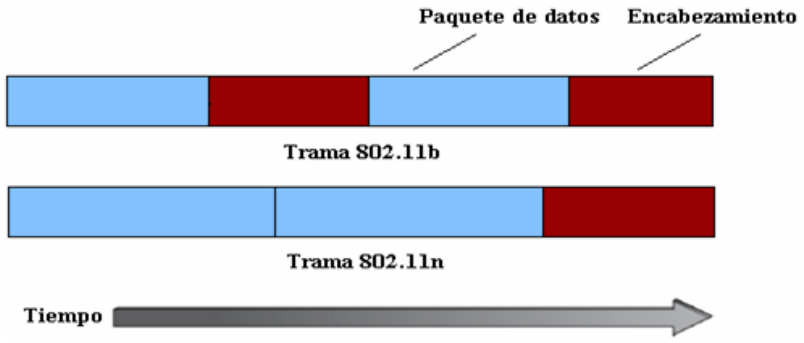


Figura 1.7: Utilización de secuencias de intercambio agregadas.

1.2 Equipamiento

El diseño e implementación de WLAN se hace sobre la base de la utilización de tres elementos fundamentales; la estación inalámbrica, el AP (*Access Point*) y el AC (*Access Controller*) [3].

El primer elemento, la estación inalámbrica, puede ser una PC (Personal Computer) o una *Laptop* con tarjeta de red inalámbrica, incorporada con el objetivo de convertir las trama *Ethernet* que genera la PC en tramas del estándar inalámbrico y viceversa. Haciendo posible la transmisión transparente de la información gracias a una o varias antenas incorporadas a dichas tarjetas.

Un AP actúa como un *hub* o concentrador, siendo el encargado de coordinar la comunicación entre las diferentes estaciones inalámbricas que están conectadas a el, además de servir como puente entre la red cableada y la red inalámbrica.

Por último el AC es un *router* IP (*Internet Protocol*) que se encarga de asignar las direcciones IP a los terminales de la WLAN, mantener la lista de direcciones de los terminales correctamente identificados y filtrar el tráfico, descartando los paquetes de terminales no autentificados. Además los AC hacen de pasarela a redes IP externas mediante su conexión a un elemento central encargado de la gestión de servicios, permitiendo la conexión a Internet y el acceso a las aplicaciones que la red inalámbrica pueda soportar.

Otro elemento que se puede encontrar en las redes inalámbricas es el WB (*Workgroup Bridge*). Este es un dispositivo que garantiza la conexión inalámbrica de una red cableada remota con un AP. También permite la conexión de dos redes LAN (*Local Access Network*) distantes mediante la utilización de antenas direccionales logrando un enlace seguro que conecte estas redes de forma directa. También se pueden encontrar repetidores cuya implementación se realiza para expandir el rango de cobertura de una WLAN [2].

1.3 Topologías Básicas

El estándar 802.11 especifica dos topologías básicas a la hora de implementar redes de área local inalámbricas [3]:

- la modalidad *Ad-hoc* o IBSS (*Independent Basic Service Set*)
- el modo infraestructura o BSS (*Basic Service Set*)

La topología *Ad-hoc* basa su funcionamiento en la comunicación entre los diferentes dispositivos inalámbricos sin que medie entre ellos ningún AP (Figura 1.8). Muchas de las responsabilidades que antes manejaba el AP son ahora manejadas por una estación. Para la comunicación entre dos estaciones sea posible hace falta que se vean mutuamente o sea que cada una de ellas este en el rango de cobertura de la otra [1]. Sin embargo en una red *Ad-hoc* donde coexistan varios dispositivos inalámbricos se puede lograr la comunicación entre dos de estos dispositivos que no se vean mutuamente mediante un tercer dispositivo que este en el rango de cobertura radioeléctrica de uno de los que se quiera comunicar y que con su propia cobertura alcance al otro [2].

Esta es una configuración flexible y sencilla de implementar donde cada estación mantiene una lista de los usuarios y contraseña de grupo y no se requiere de ningún tipo de gestión administrativa pero requiere de un número no elevado de terminales, control de potencia que evite la interferencia y está limitada por el rango de cobertura de las NIC (*Network Interface Card*) para establecer el enlace [3].

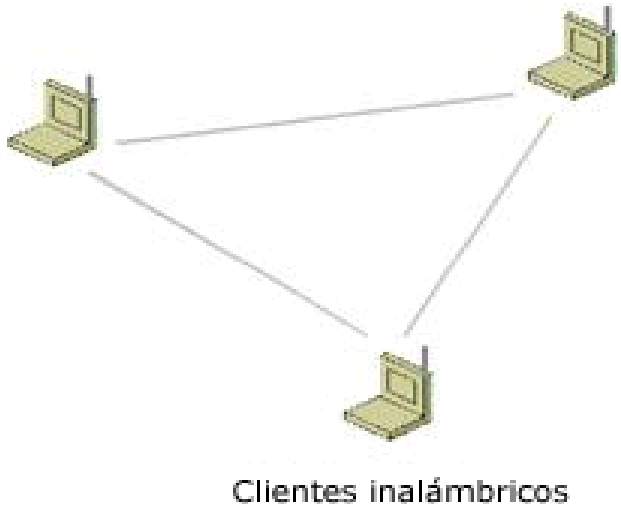


Figura 1.8: Red Ad-hoc.

El modo infraestructura amplía una red cableada existente con dispositivos inalámbricos mediante la utilización de un AP que actúa como controlador de la red inalámbrica. El rango de cobertura está condicionado por el alcance del AP. En este modo se pueden diferenciar dos partes, el BSS y el ESS (*Extended Service Set*) [3].

El primero se caracteriza por un conjunto de estaciones inalámbricas que compiten para acceder al medio compartido que ofrece el AP. La conexión al *backbone* de la red externa la realiza el mismo AP. Cada celda BSS que depende de la cobertura del AP debe estar aislada del resto con el fin de evitar interferencias.

El segundo se caracteriza por tener más de dos BSS conectadas mediante un DS (*Distribution System*), alámbrico o inalámbrico (Figura 1.9).

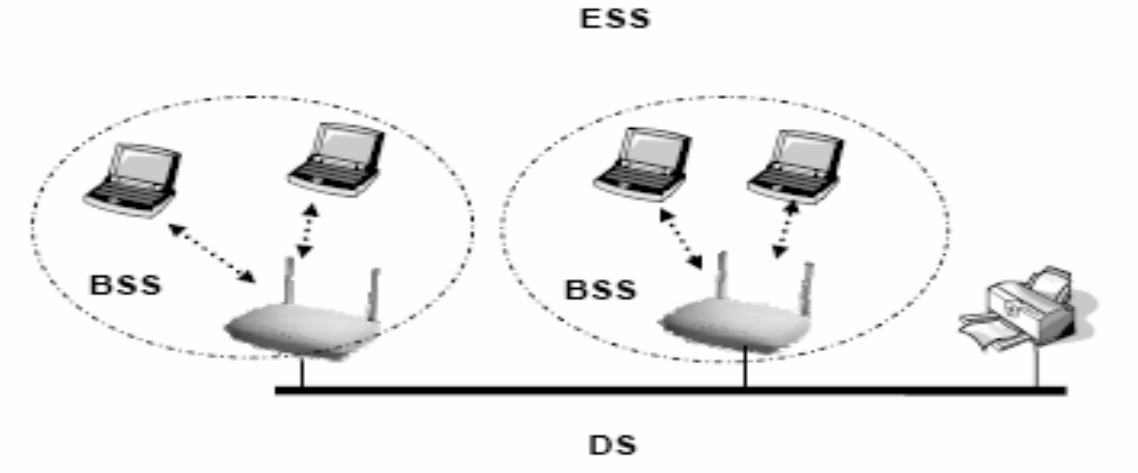


Figura 1.9: Modo Infraestructura.

1.4 Seguridad

Desde su creación, 802.11 ha brindado algunos mecanismos básicos de seguridad donde las primeras soluciones vinieron dadas por la configuración de los AP mediante un identificador de conjunto de servicio que puede considerarse como el nombre de la red. Este identificador debe ser conocido por la tarjeta de red para así relacionar la estación inalámbrica con el AP y proceder a la transmisión y recepción de los datos de la red [3].

Otro mecanismo empleado fue el WEP (*Wired Equivalent Protocol*), solución implementada sobre la capa MAC (*Media Access Control*) que otorga una técnica de encriptación adicional basada en un algoritmo RC4 que comprime y encripta los datos que se van a trasmitir [7].

Posteriormente la IEEE adapta el estándar 802.1x para redes Wi-Fi, en el se brinda un mecanismo de control y de seguridad basado en acceso a redes inalámbricas mediante puertos. Con los mecanismos anteriores solo se autentificaba al dispositivo mientras que con este se hace necesario autentificar al usuario. Este estándar define tres elementos, el servidor de autentificación donde se verifican las credenciales del usuario, el autenticador que es el dispositivo en el que se recibe la información del usuario y la traslada al servidor de autentificación,

y el suplicante que es el dispositivo que provee las credenciales del usuario al autenticador [14].

En el año 2003 es lanzado WPA (*Wi-Fi Protected Access*), creado especialmente para lidiar con los problemas de WEP. En el se provee de un sistema de encriptación más fuerte en el cual se puede utilizar una clave privada compartida o claves únicas asignadas a cada usuario para autentificar el punto de acceso y el cliente. WPA utiliza el protocolo TKIP (*Temporal Key Integrity Protocol*) donde las claves se pueden rotar rápidamente reduciendo la posibilidad de que una sesión sea descifrada. El proceso de autentificación se realiza consultando una base de datos externa mediante el protocolo 802.1x [11].

Actualmente el protocolo de seguridad más avanzado es WPA2 que es una mejora relativa a WPA. WPA2 se basa en el estándar 802.11i para seguridad de WLAN donde se abarca los protocolos 802.1x, TKIP y AES (*Advanced Encryption Standard*) [5].

1.5 Radiopropagación

El término de radiopropagación no es más que la propagación de las ondas electromagnéticas vía radio frecuencia. La situación del trayecto de propagación respecto a los obstáculos, las características eléctricas del terreno, las propiedades físicas del medio, la frecuencia y polarización de la onda electromagnética, influyen de manera directa en las características de propagación de las mismas [15].

Según la frecuencia, pueden distinguirse los modos de propagación por:

- Onda de Superficie para frecuencias inferiores a 30 MHz.
- Onda Ionosférica para frecuencias entre los 3 y los 30MHz.
- Onda Espacial para frecuencias superiores a los 30 MHz.
- Onda de Dispersión Troposférica.

1.6 Conceptos

Para el estudio de las redes WLAN, es necesario explicar algunos conceptos, que sientan las bases para el posterior análisis y dimensionamiento de un enlace.

Clasificación de los entornos: Se clasifican atendiendo a varios parámetros:

- Para medir el rendimiento de una red WLAN es necesario analizar el entorno físico circundante, en cuanto al entorno físico se clasifican en elementos estáticos y dinámicos.
- Por las cualidades del entorno se clasifican: en interior (*indoor*) o exterior (*outdoor*).
- Con respecto al análisis de la zona de cobertura, este se subdivide en otras áreas de menor tamaño o células, y la clasificación está en dependencia de su radio, existen las macro-células pequeña y extensa, micro-célula y pico-célula.

Zona de Fresnel: Se definen como las formas elípticas o elipsoides (elipse en revolución) que rodean la trayectoria visual entre el emisor y el receptor de una onda electromagnética sin obstrucción. Estas zonas quedan establecidas porque la propagación de las ondas de radio entre los dos puntos, no es en línea recta, debido a consideraciones de dispersión. Las dimensiones de las zonas de Fresnel varían en dependencia de la longitud del recorrido y la frecuencia de la señal. El radio de las zonas de Fresnel se calcula como sigue:

$$R_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}} \qquad (1.1)$$

El término n dentro de la expresión, se refiere a una zona determinada, por ejemplo para calcular el radio de la primera zona de Fresnel $n = 1$. Los términos d_1 y d_2 se refieren a las distancias del transmisor al obstáculo más crítico, y de este último al receptor (Fig. 1.10). En la expresión la suma de d_1 y d_2 se refiere la

distancia que hay entre los puntos del enlace, que viene representada en la figura por D.

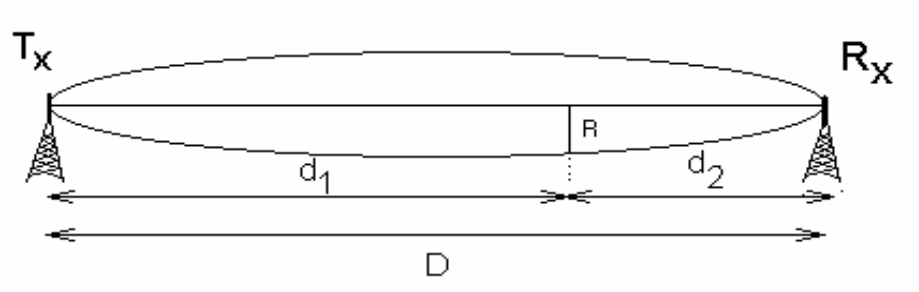


Figura 1.10. Primera zona de Fresnel.

En la práctica es necesario que al menos el 60% de la primera zona de Fresnel esté libre de obstáculos. La tabla 1.1 muestra los diferentes valores de atenuación en función de la clarencia, que es la distancia de la obstrucción a la línea de visión y se mide en metros, que pueden dificultar la calidad de la señal que se transmite.

Tabla 1.1 Atenuación en función de la clarencia.

ZONAS DE FRESNEL	ATENUACION
0.5 zone clear	2 dB
0 (touching)	6 dB
0.5 zone obstructed	10 dB
1.0 zone obstructed	16 dB
1.5 zone obstructed	19.5 dB
2.0 zone obstructed	22 dB
2.5 zone obstructed	24 dB
3.0 zone obstructed	25.5 dB

Finalmente otros parámetros relacionados con este tipo de redes son:

LOS (Line-of-sight), línea visual: Es una línea imaginaria que existe entre el transmisor y el receptor de forma tal que ambos se vean. La línea visual que se necesita para tener una conexión inalámbrica óptima, desde el trasmisor hasta el receptor, es más que simplemente una línea delgada, su forma es parecida a un elipsoide.

NLOS (Non-Line-of-sight), fuera de la línea visual: Se produce cuando entre el transmisor y el receptor la visibilidad es bloqueada totalmente.

OLOS (Obstructed-line-of-sight), línea visual obstruida: Ocurre, cuando parte de la línea visual queda obstruida de forma parcial por un objeto.

Para enlaces punto a punto se busca siempre la forma de que operen en condiciones de LOS, con un despeje de la zona de Fresnel de al menos un 60%, en interiores no es necesaria la existencia de líneas de Vista, y pueden operar en condiciones de NLOS lo que los alcances o las velocidades que se logran son menores, ya que las perdidas de propagación aumentan, debido a la degradación del enlace por la no existencia de LOS, lo ideal es que siempre exista LOS, pero pueden operar en cualquiera de las tres condiciones.

1.7 Mecanismos de propagación

Las señales electromagnéticas se propagan por medio de varias formas entre una antena transmisora y una receptora. Si el medio en que se propagan fuera totalmente uniforme las ondas, se moverían en línea recta. Para las frecuencias de SHF donde la ionosfera se hace transparente, la propagación en espacio libre es modificada por el suelo (reflexión y difracción) y por la troposfera (refracción, absorción y dispersión).

Reflexión, Refracción y Absorción

Primeramente las ondas provenientes de un medio inciden sobre la superficie de otro, parte de la energía de la ondas se refleja (cambio en la dirección de propagación) dentro del primer medio, a la vez que otra parte de la energía es transmitida o refractada (cambio en la dirección de propagación producto de cambio de un medio a otro) en el segundo, y por otro lado una tercera porción se absorbe (cuando las ondas electromagnéticas atraviesan algún material). Mientras los conductores perfectos reflejan toda la señal, otros materiales reflejan sólo parte de la energía de la onda incidente y transmiten el resto.

Interferencia, ruido y distorsión

En las redes WLAN el medio en que se transmite, el aire, introduce pérdidas y diferentes tipos de perturbaciones a pesar de que el transmisor y el receptor, unidos a sus antenas hacen posible la comunicación. Entre las perturbaciones se encuentran: interferencia, ruido y distorsión que atentan contra la originalidad de la onda que llega al receptor proveniente del transmisor. Múltiples son las fuentes de ruido, interferencia y distorsión.

Interferencia

La interferencia es un tipo de perturbación que afecta el buen funcionamiento de un sistema radioeléctrico. Las interferencias según [15], se pueden clasificar en dependencia del número de fuentes: en simples, cuando hay una sola señal interferente y en múltiples, cuando existen varias fuentes interferentes. También se distinguen entre interferencia cocanal y de canales adyacentes. [16]

Ruido

Es la señal no deseada presente siempre en un sistema eléctrico, influye de manera negativa en la capacidad del receptor limitando la velocidad del enlace, puede ser provocado por fuentes naturales y artificiales. Las fuentes naturales se clasifican en externas e internas al sistema.

- **Ruido Natural:** Las fuentes de ruido se deben a la radiación producida por elementos naturales: tierra, cielo, considerados como cuerpos negros y los efectos del medio (lluvias, gases atmosféricos sobre esta radiación).
- **Ruido Artificial o Industrial:** Este tipo de ruido aparece como consecuencia de diferentes actividades de carácter industrial, así como la tracción de vehículos, transporte y distribución de energía eléctrica, entre otros. El espectro del ruido artificial disminuye al aumentar la frecuencia.
- **Ruido Térmico:** Este tipo de ruido es producido por el movimiento de las cargas libres en los conductores debido a su agitación térmica, se presenta en

amplificadores, atenuadores y en cuadripolos, además, de que puede ser captado por la antena [17].

Distorsión

Se define la distorsión como la relación de las potencias medias de error y de señal. Es la diferencia entre la señal que entra a un equipo o sistema y la señal de salida de mismo. Puede definirse también como la deformación que sufre una señal tras su paso por un sistema. La distorsión puede ser lineal o no lineal. Para el caso de las redes WLAN, se manejan los términos de Distorsión por Intermodulación y por Multitrayecto. [18]

Distorsión por Intermodulación**:** Distorsión no lineal en un sistema, caracterizada por la aparición en la salida de frecuencias que son combinaciones lineales de las frecuencias fundamentales y sus armónicos presentes en la señal de entrada [19].

- Distorsión por Mulitrayecto**:** Se produce cuando diversas ondas con variaciones respecto a la original, viajan por múltiples trayectorias hasta llegar al receptor. Para reducir la distorsión conocida como pérdidas por multitrayecto debido a reflexiones se utilizan los sistemas de diversidad.

1.8 Conclusiones

Los aspectos analizados en el capítulo I son la base teórica para el diseño de enlaces inalámbricos. Para ello primeramente es necesario hacer la concepción teórica del enlace para luego escoger el tipo de topología que se va a usar y definir el estándar que cumple con los requerimientos técnicos según la norma, la banda de frecuencia donde van a operar los equipos de radioenlace, las velocidades y ancho de banda del canal, el mecanismo de acceso al medio que se implementa sobre la capa MAC y las técnicas de modulación de la señal empleadas para lograr la mejor calidad del enlace.

En cuanto a las técnicas de radio propagación debemos calcular: la zona de Fresnel, el tipo de antena que es mejor usar según el área de cobertura que se necesita cubrir con el enlace además del cálculo de las potencias en el equipo de

transmisión y recepción incluyendo las perdidas en la transmisión y la sensibilidad del receptor. Todos estos aspectos definen posteriormente el tipo de equipamiento a usar y nos garantizan calidad y estabilidad en el enlace diseñado.

También se analizaron aspectos muy importantes de seguridad y control de acceso de los usuarios que son necesarios para lograr en el equipo de radio usado la mayor confidencialidad posible en la transmisión de los datos.

La descripción realizada a lo largo de este trabajo de las tecnologías empleadas en el estándar IEEE 802.11n ha propiciado que se tenga un panorama bastante amplio de lo que el mismo puede ofrecer. Aun así, y dada la relevancia que se prevé adquiera este tipo de redes, se mencionan algunas cuestiones importantes que se deben considerar a la hora de implementar las mismas:

Las velocidades alcanzadas por redes 802.11n constituyen un gran atractivo para los consumidores, sin embargo, la velocidad de una red inalámbrica la fija el usuario más lento, por lo que solo en algunos casos se podrá sacar ventaja de la velocidad [9].

El uso de canales de 40MHz permite un mejor rendimiento y reduce la complejidad de una red 802.11n, sin embargo, allí donde la disponibilidad del espectro sea escasa, su utilización puede verse limitada [9].

La compatibilidad de 802.11n con los estándares 802.11a/g significa un gran sacrificio de recursos técnicos ya que los entornos que limitan el ancho del canal a 20MHz serán sobrecargados con los costos adicionales de implementaciones MIMO complejas a fin de lograr el rendimiento requerido [9].

Capítulo II

CAPÍTULO II. PROYECTO DE SUBRED INALÁMBRICA

El diseño de una Red Inalámbrica depende significativamente del objetivo del proyecto. En algunos casos se busca movilidad de los usuarios, o disminuir los costos. Independientemente de cuál sea la motivación, siempre hay que lograr una buena productividad de los usuarios, lograr un mínimo de seguridad y que la calidad de servicio sea similar a las redes cableadas**,** si tenemos en cuenta que estas usan como medio compartido el aire para transmitir ondas de RF, y que existen obstáculos e interferencias que afectan la calidad del enlace, de ahí que es de vital importancia para desplegar una red inalámbrica hacer primeramente un estudio del entorno y el terreno, algo que debe hacerse periódicamente pues las condiciones cambian con el tiempo. La finalidad de este estudio es determinar el lugar óptimo de emplazamiento de los puntos de acceso y detectar los obstáculos, que influirán en la calidad de la red. Estos deberán ser tenidos en cuenta al diseñar esa red específica y asegurar una cobertura adecuada a todos los usuarios. Además se debe tener en cuenta según el equipamiento a emplear la potencia de la señal, las antenas que se utilizan y sus características y las pérdidas que se producen debido a la propagación.

2.1 Bases para la proyección

Para el diseño de una red inalámbrica o WLAN se debe ser muy cuidadoso y cumplir lo más fielmente posible con una serie de pasos o metodología existente para este fin, ya que como se aprecia en capítulos anteriores, las necesidades de los usuarios finales cada día son más exigentes, en cuanto a calidad de servicio, seguridad, velocidad entre otras características. También en el capítulo anterior se afirma que la velocidad de una red inalámbrica la define el elemento más lento de la red.

2.1.1 Requerimientos básicos

Los sistemas de conectividad inalámbrica deben cumplir con características propias o cercanas a las redes cableadas que permitan:

Altos Rendimientos

Evitar que se conviertan en un cuello de botella. Tener en presente que las velocidades en las redes cableadas oscilan desde los 100 Mbps (*Fast Ethernet),* 1.000Mbps *(Gigabit Ethernet),* hasta velocidades del orden de los 10.000Mbps *(10 Gigabit Ethernet).*

Crecimiento acelerado en la potencia de la informática móvil y la riqueza de los contenidos en red cada día más orientados a la transmisión de audio y video, servicios que demandan un gran ancho de banda y altas velocidades de transmisión.

Movilidad y *Roaming*

Aunque siempre han existido los usuarios móviles, sólo ahora pueden estar conectados mientras se desplazan de un lugar a otro sin necesidad de que el usuario realice alguna operación para ello.

Dotar de la suficiente inteligencia a los sistemas de redes inalámbricas es una cuestión crítica a la hora de dar soporte a usuarios móviles, a fin de que estén conectados sin interrupciones del servicio.

Seguridad

La necesidad de tener en cuenta la seguridad de estas redes viene dada por la sencilla razón de que la naturaleza de la transmisión no impone fronteras, ya que la misma utiliza como medio de propagación el aire. Por tanto la transmisión de señales inalámbricas no puede ser limitada enteramente al espacio privado de una empresa o del hogar.

Por lo tanto las WLAN han de contar con sistemas de seguridad fiables y sencillos para el usuario final.

Gestión

Para garantizar el rendimiento, la movilidad y la seguridad, es fundamental proporcionar las herramientas apropiadas para configurar estas opciones o servicios, monitorizar las redes inalámbricas y así poder localizar y solucionar problemas en las mismas.

Cobertura

La red inalámbrica debe estar disponible en todas las instalaciones del espacio que se desea cubrir con el enlace.

Estándar

Es importante establecer qué normas gobernarán el funcionamiento, tomando en cuenta modos de operación, frecuencia de trabajo, tipo de modulación, tasa de transferencia, niveles de seguridad, cobertura, además de considerar, la presencia en el mercado de dispositivos de redes WLAN, para así asegurar la interoperabilidad de los componentes.

Modos de Operación y Topología

Se debe definir cual de los modos de operación básicos existentes se va a usar en el diseño: *Ad-Hoc* ó Insfraestructura. Teniendo en cuenta que la topología es la configuración que pueden tomar los dispositivos que componen la WLAN. Dentro de las topologías más comunes tenemos:

1. Un AP con múltiples clientes.
2. Dos o más AP con múltiples clientes practicando *roaming.*
3. Extensión del alcance WLAN utilizando AP como repetidores.
4. Extensión del alcance WLAN utilizando antenas repetidoras.
5. Enlace entre dos segmentos de red con AP o antenas direccionales, topología *bridge.*

Flexibilidad y Escalabilidad

La flexibilidad es la capacidad de la red de cambiar rápida y fácilmente de topología física, es decir, que los equipos presentes en la red, tanto AP como estaciones clientes no estén atados a una posición fija.

Por otra parte la escalabilidad es la propiedad de una red de crecer y ampliar su rango de cobertura y/o número de usuarios sin alterar su configuración y topología.

Características de la señal

Debido a su naturaleza, las señales de radio frecuencia pueden verse afectadas, desvanecerse o bloquearse por los características propias de los distintos materiales de construcción y del entorno, así como por efectos ambientales.

En la tabla 2.1 podemos observar los elementos o factores ambientales y materiales de construcción más comunes que afectan negativamente a la señal inalámbrica.

Tabla 2.1 Elementos que afectan negativamente a la señal inalámbrica.

Material	**Ejemplo**	**Interferencia**
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia, niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de Papel	Alta
Vidrio con alto contenido de plomo	Ventanas	Alta
Metal	Vigas, armarios	Muy alta

Sistema de seguridad

Cuando la WLAN forma parte de una red corporativa, abre un espacio por el cual un usuario puede saltarse los sistemas tradicionales de seguridad, por ejemplo un cortafuego, ingresar al *backbone* principal de la red, tener acceso a los elementos que forman la red ya sean servidores, *routers*, o estaciones de trabajo. Ver Figura 2.1.

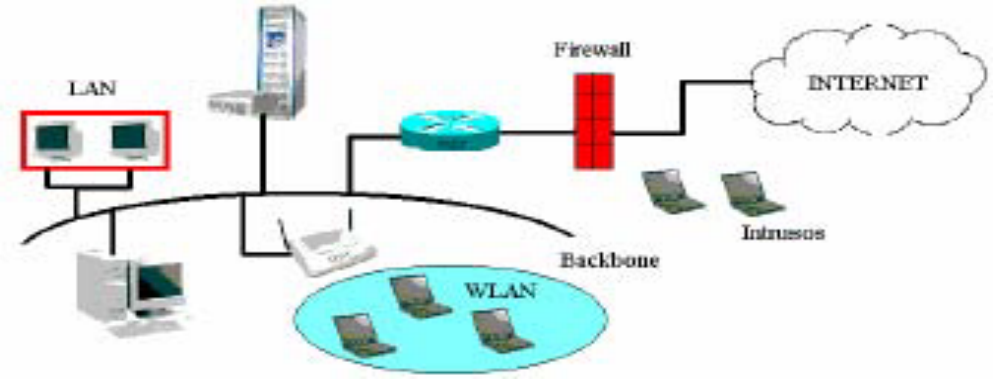


Figura 2.1. Sistema de seguridad.

Como solución al problema descrito, se debe implementar los sistemas de seguridad propios de las redes WLAN, complementados con sistemas de seguridad tradicionales, de las redes cableadas tales como:

1. SSID: *Service Set* ID.
2. *Autentificación Shared Key*.
3. WEP: *Wired Equivalent Privacy*.
4. WPA o WPA2: Servicio de usuario de marcado con autenticación remota (RADIUS)
5. Filtrado de direcciones MAC.
6. Cortafuego entre el AP y el *backbone* de la red.
7. Redes Privadas Virtuales (VPN).

Sistema de administración

Proveer los servicios necesarios para que el usuario final pueda utilizar la red en forma cómoda y segura. Entre los servicios fundamentales tenemos la asignación dinámica de direcciones de red, mediante servidor DHCP, el acceso a la red principal, a través de un *Router*, la protección de la red con un cortafuego. La gran mayoría de los dispositivos inalámbricos que existen en el mercado hoy en día ya sean AP o *Routers*, cuentan con la capacidad de prestar estos servicios. Una alternativa, es implementar una máquina externa con los servicios necesarios para realizar la gestión de la red.

Diseño de la Red

La primera tarea es conseguir un plano de planta de la construcción del lugar en el cual se quiere instalar la red inalámbrica. Luego, en el plano, se realiza un estudio, para definir la ubicación y cantidad de AP necesarios para cubrir el área deseada. Este procedimiento es conocido como *Site Survey* (Análisis del lugar).

El objetivo fundamental es suministrar la suficiente información para determinar la ubicación y el número de AP que se deben instalar para proporcionar la cobertura adecuada. Además de detectar la presencia de fuentes de interferencias y la existencia de otras redes inalámbricas que podrían degradar el funcionamiento de la red a instalar.

Esto se logra utilizando las denominadas "*Site Surveys Tools*": herramientas que ayudan a comprobar el alcance y calidad de los enlaces inalámbricos Wi-Fi. Dentro de estas herramientas se consideran: el software incorporado en las NIC inalámbricas y un analizador de espectro.

2.2 Equipamiento para el enlace

Para acometer el enlace de lo que sería la red WLAN se dispone de 3 AP, y cable UTP 6.

Los AP de que se dispone para el enlace serán de la marca D-Link el modelo DWL-2000AP+ que entre sus especificaciones técnicas principales cuenta:

Estándares	IEEE 802.11g IEEE 802.11 IEEE 802.11b IEEE 802.3 IEEE 802.3u
Rango de frecuencias	2.4GHz to 2.4835GHz
Velocidad de Datos	54 Mbps
Potencia de Transmisión	11g: 14dBm 11b: 16dBm
Seguridad	802.1x WPA (TKIP, MIC, IV *Expansion, Shared Key Authentication*)
Tipo de antena (ganancia)	2.0 dBm con conector SMA
Técnicas de utilización del medio	OFDM CCK PBCC
Acceso al medio	CSMA/CA con ACK
Modos de operación	AP Cliente Puente (Bridge) Multi punto
Requerimientos de sistema	*Internet Explorer* o *Nestcape* versión 6 ó superior
Temperatura de Operación	*$0^{o}C$ a 55 ^{o}C*

2.3 Proyecto para la Red WLAN CCB

Según la metodología descripta en el epígrafe 2.1 para realizar el diseño de una red inalámbrica debemos cumplir con una serie de pasos que describiremos a continuación.

Paso 1: Adquirir un plano del lugar.

En el centro de Convenciones Bolívar se dispone del plano del lugar, donde se aprecia claramente la ubicación de todas las áreas. Esto constituye un elemento esencial para continuar con los siguientes pasos del proceso. En la figura 2.2 se aprecia el plano del lugar.

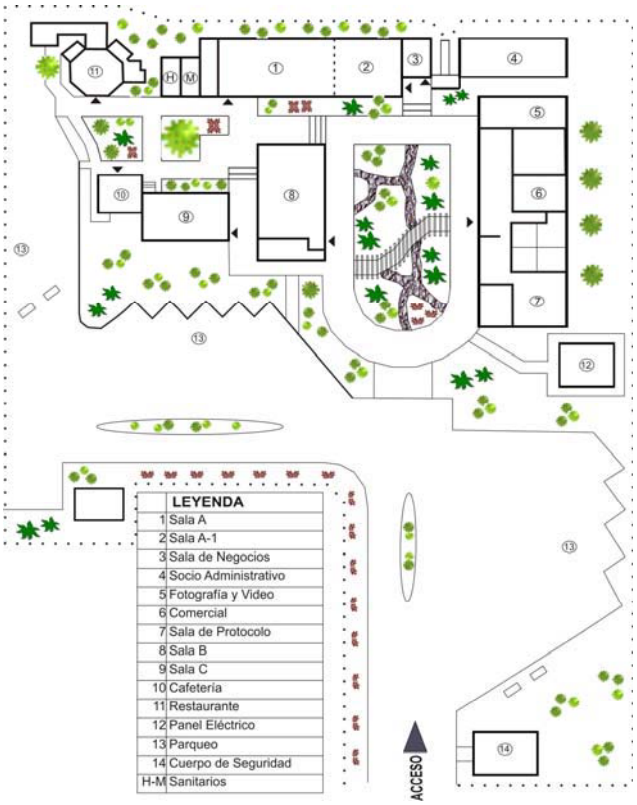


Figura 2.2. Plano del lugar.

Paso 2: Inspección visual.

Al inspeccionar y evaluar en forma visual el sector que se desea cubrir con la WLAN se puede determinar la existencia de obstáculos que no aparezcan en el

plano. También identificar posibles fuentes de atenuación e interferencias de radiofrecuencias y considerar si existen elementos y/o características del lugar que degraden el funcionamiento de la red WLAN.

En este caso particular se distinguen, según lo descrito en la bibliografía que las fuentes posibles de atenuación de la señal o interferencias pudieran estar dadas por los materiales de construcción utilizados en las edificaciones a base de paredes de ladrillos, mampostería, ventanales de cristal y soluciones de techo usando estructuras metálicas (cerchas) para soportar madera y tejas de barro.

Además de estos materiales otros elementos que inciden en la calidad de la señal lo constituyen las ramas de árboles y arbustos que rodean el lugar, donde predominan los jardines a todo el rededor del lugar.

Todos estos elementos identificados en la inspección visual afectan o degradan de alguna forma la calidad de la señal como se observa mas adelante, el grado de afectación de los mismos se aprecia en la tabla 2.1.

Paso 3: Identificación del área de cobertura.

En este paso como bien lo dice el título se procede a marcar o seleccionar las áreas a las cuales se quiere dar cobertura con la red inalámbrica. Nuevamente mediante el plano del lugar se ubica en él según muestra la figura 2.3 las áreas que se quiere cubrir con el enlace.

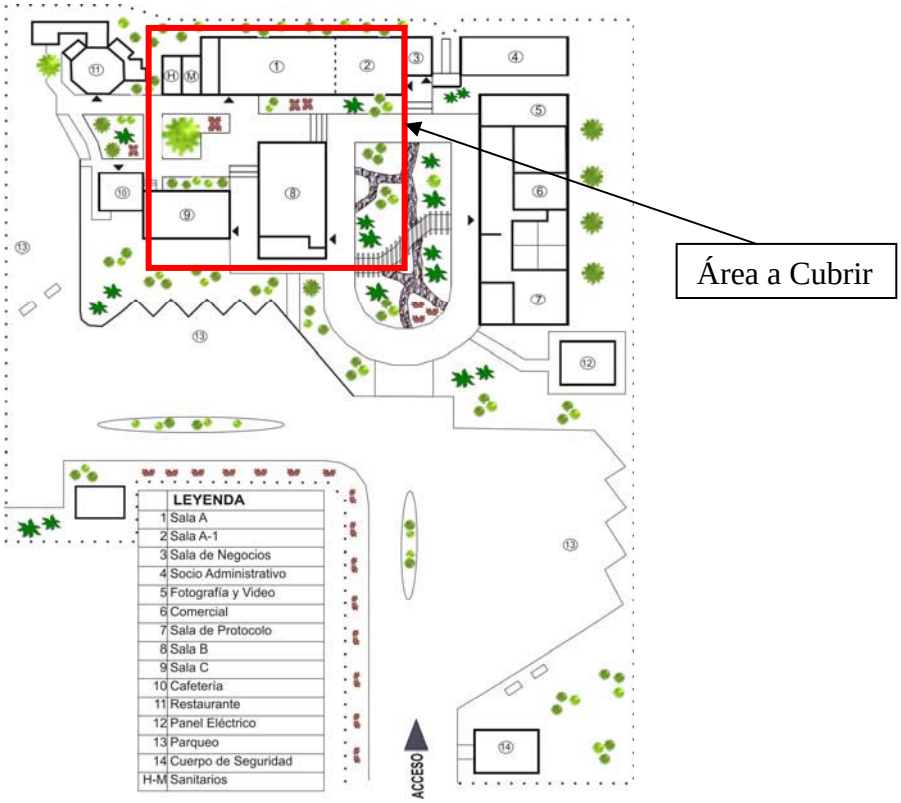


Figura 2.3. Áreas a cubrir con la red inalámbrica.

Paso 4: Ubicación preliminar de los AP.

Teniendo en cuenta las características de los APs disponibles, en cuanto a potencia de transmisión, tipo de antena, disponibilidad de red eléctrica, disponibilidad de red de datos y alcance del AP, se propone colocar uno lo más al centro de la zona que se desea dar cobertura, nominalmente los AP logran un alcance en: Interiores (*Indoor)* de 100m y en exteriores (*Outdoor)* de 400m. Los APs que se dispone son del tipo *indoor* es decir para interiores y con esto se comienza a realizar pruebas monitoreando la señal.

En la figura 2.4 se muestra el lugar escogido preliminarmente para colocar el AP.

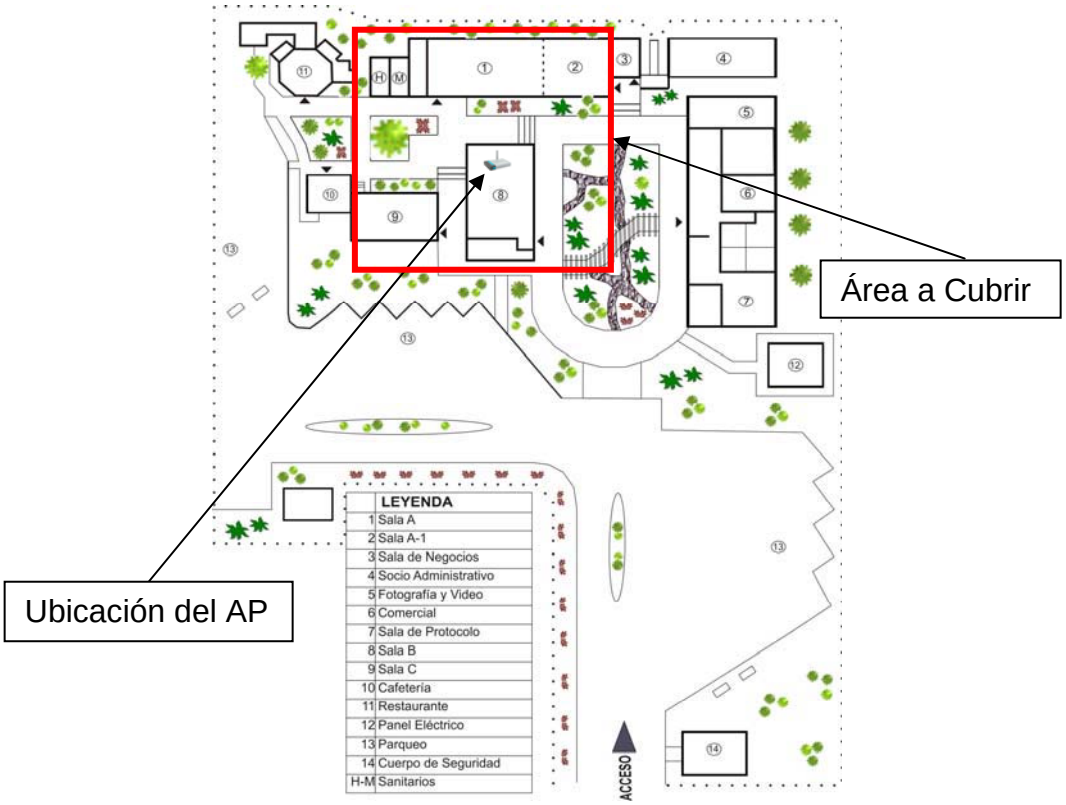


Figura 2.4. Ubicación preliminar del AP.

Paso 5: Verificar la ubicación de los AP.

Para verificar si con esta ubicación preliminar para el AP se logra dar cobertura al área deseada se comienza a monitorear mediante una herramienta del tipo *"Site Survey Tool"*, en este caso con el *software Xirrus Wifi Inspector* , ver figura 2.5.

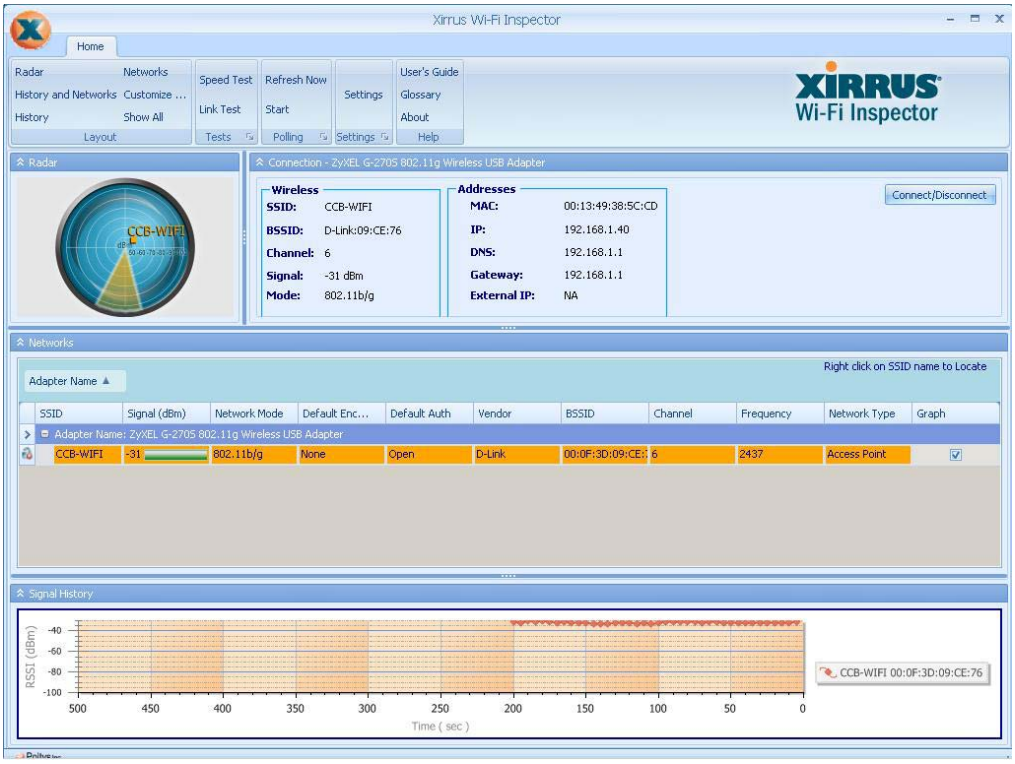


Figura 2.5. Xirrus WiFi Inspector. Software del tipo "Site Survey Tool".

Mediante el uso de esta herramienta y el de una maquina móvil a medida que se aleja del AP se recopilan los datos que arroja el *WiFi Inspector* en cuanto a Velocidad del enlace (*Tx Rate*), calidad del enlace (*Quality of Link*) y fuerza de la señal (*Signal Strength*). Con las mediciones recopiladas en los diferentes puntos se conforma la tabla 2.2.

Tabla 2.2 Resultados experimentales de cobertura.

Distancia (m)	Velocidad del enlace (Mbps)	Calidad del enlace (dBm)	Fuerza de la señal (%)
8	54	-36	98
16	48	-38	95
24	48	-46	90
32	48	-54	84
40	36	-72	76
48	36	-76	60
50	32	-80	54

Paso 6: Documentación.

En este momento se da a conocer los datos exactos de ubicación del AP, en cuanto a altura, requerimientos eléctricos y de datos, la topología física y lógica de la red, el modo de operación y el rendimiento.

En este caso no se da datos concluyentes en este momento, pues en el siguiente epígrafe se analiza de acuerdo a las mediciones realizadas, que determinación tomar.

2.4 Análisis del sistema proyectado

Según los datos que arrojan las mediciones realizadas con la ubicación preliminar del AP, se aprecia que los materiales de construcción empleados en las edificaciones de las áreas que se necesita cubrir, así como la cantidad de árboles y arbustos que la rodean afectan de manera media a alta a la señal, ya que al alejarse unos pocos metros del AP la misma comienza a perder calidad y velocidad, si solo permanecían 2 usuarios conectados a la red al mismo tiempo, esto se vería seriamente afectado cuando aumente el número de usuarios conectados al unísono y comience a circular paquetes de datos incrementando el tráfico, por lo que se determina ubicar mas APs, logrando mejores resultados cuando se ubican 3 AP para cubrir el área antes mencionada, dichos APs fueron nuevamente probados partiendo del paso número 1 del procedimiento, es de destacar que fueron programados en canales no solapados. Si se parte del análisis de la figura 2.1. En la misma se observa 11 canales solapados y 22 MHz de ancho de banda por canal.

Entonces 3 puntos de acceso o AP pueden ocupar la misma área o partes de la misma área a cubrir si colocamos cada uno en canales no solapados, por ejemplo en el canal 1, 6 y 11. La ubicación de los APs queda dispuesta según lo muestra la figura 2.6.

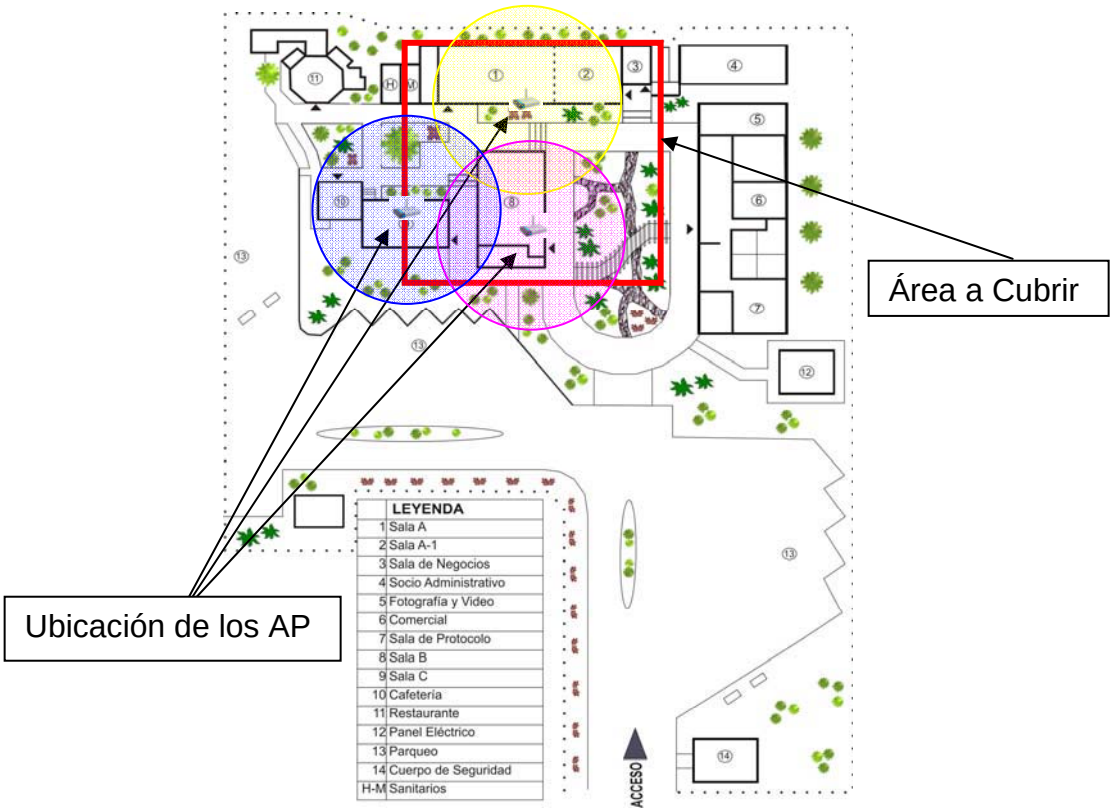


Figura 2.6 Ubicación de los AP según un área de cobertura efectiva de 24 metros.

Luego de colocarse los 3 AP como se muestra en la figura 2.6 nuevamente se realizaron mediciones lográndose mejores resultados, en cuanto a alcance de la señal y tasas de transferencia de datos, redundando esto en una mejora sustancial en la calidad del enlace, el anexo VI muestra algunos resultados de las mediciones realizadas al respecto.

2.5 Conclusiones

El detallado estudio de las condiciones del terreno donde se deseó establecer el enlace, la situación existente en la red CCB con respecto a aquellas áreas del centro fuera del alcance de la misma, constituyeron aspectos necesarios para la decisión de cómo interconectar estos lugares, y posteriormente seleccionar el equipamiento a utilizar. Teniendo en cuenta que los cálculos teóricos que se han hecho cumplen con los requisitos técnicos que se exigen para el calculo de los sistemas de radio enlace se decidió asumir el proyecto de montaje para llevar los

recursos de la red a las áreas que necesita con urgencia de todos los servicios que se ofrecen para lograr sus objetivos científicos y sociales.

Es preciso a la hora de realizar el diseño de una subred inalámbrica del tipo WLAN, seguir la siguiente metodología o pasos:

- Paso 1: Adquirir un plano del lugar.
- Paso 2: Inspección visual.
- Paso 3: Identificación del área de cobertura.
- Paso 4: Ubicación preliminar de los AP.
- Paso 5: Verificar la ubicación de los AP.
- Paso 6: Documentación.

Capítulo III

CAPÍTULO III. CONFIGURACIÓN DE LA WLAN Y SU ENLACE CON LA RED ETHERNET DEL CENTRO

Como parte de la puesta en marcha del enlace analizaremos los aspectos técnico-prácticos y administrativos más importantes que son necesarios para lograr la mayor seguridad y el mejor rendimiento posible de la red.

3.1 Descripción de los protocolos de red que se usan en la configuración de las redes WLAN

Para la configuración de los protocolos de red se debe partir del hecho de conocer cuales de los protocolos de redes sería necesario implementar y configurar para que la red inalámbrica funcione adecuada y eficientemente.

Lo primero es definir el modo en que va a operar el AP, ya sea como punto de acceso, repetidor, puente de enlace, entre otros modos, luego es necesario configurar el AP de tal modo que este tenga un nombre para identificarlo (AP *name*) y también definir como se llama la red a la que va a pertenecer (SSID *name*). Se debe definir en este paso en que canal va a transmitir el AP.

Posteriormente corresponde colocar o definir el protocolo de red que se va a usar, es decir asignar el IP que va a identificar el AP dentro de la red, esto puede hacerse de dos formas, una que el AP lo adquiera de un servidor DHCP o en su defecto configurar el servidor DHCP propio del AP, y la otra asignar una IP estática con su correspondiente máscara de red y su puerta de enlace con la red.

3.2 Configuración de los protocolos para redes WLAN según características propias de la red CCB

Para la configuración de los protocolos de la red inalámbrica se asume que la red CCB cuenta con un servidor de dominio, existe un servidor DHCP para otorgar las

direcciones IP a los usuarios, están instalados también un servidor DNS y un servidor RADIUS.

Se decide asignar a los AP direcciones IP estáticas para un mejor control en el momento de la gestión y administración de dichos dispositivos.

Como paso número 1 se asigna el nombre a cada AP, el nombre de la Red WiFi, el modo de operación y el canal en que va a operar cada AP que queda como sigue:

Nombre AP	Nombre de la RED	Modo de operación	Canal en que opera
Sala A	CCB-WiFi	Punto de acceso	1
Sala B	CCB-WiFi	Punto de acceso	6
Sala C	CCB-WiFi	Punto de acceso	11

Como segundo paso se define la dirección IP de cada punto de acceso, así como la máscara de red y la puerta de enlace, que queda a modo de ejemplo de la siguiente manera.

Nombre AP	Dirección IP	Mascara	Puerta de enlace
Sala A	192.168.1.40	255.255.255.0	192.168.1.1
Sala B	192.168.1.41	255.255.255.0	192.168.1.1
Sala C	192.168.1.42	255.255.255.0	192.168.1.1

Como tercer paso se define el protocolo de seguridad y autenticación de usuarios que en este caso sería para la seguridad el protocolo WPA vinculado al protocolo de autenticación de usuarios RADIUS, ya que existe un servidor de dominio en la red con estos servicios implementados. En el epígrafe 3.3.2 se hace una explicación detallada de cómo configurar un servidor RADIUS.

En el anexo VII se observan algunas imágenes de la configuración de uno de los AP de la red inalámbrica.

3.3 Seguridad en redes WLAN

Uno de los problemas más graves a los cuales se enfrenta la tecnología inalámbrica, es la seguridad. Estas redes son inseguras por el medio de transporte que emplean. Desde su creación, 802.11, se han implementado diversos mecanismos básicos de seguridad. [20]. A continuación se profundiza en aspectos contenidos dentro de la seguridad en este tipo de redes.

3.3.1 Riesgos de las redes inalámbricas

La topología de estas redes consta de dos elementos claves, las estaciones cliente (STA) y los puntos de acceso (AP). La comunicación puede realizarse directamente entre estaciones cliente o a través del AP. El intercambio de datos sólo es posible cuando existe una autentificación entre el STA y el AP y se produce la asociación entre ellos (un STA pertenece a un AP). Por defecto, el AP transmite señales de gestión periódicas, la STA las recibe e inicia la autentificación mediante el envío de una trama de autentificación. Una vez realizada ésta, la estación cliente envía una trama asociada y el AP responde con otra. [21]

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma. Sin embargo los asuntos más inmediatos para las comunicaciones inalámbricas son el robo de dispositivos, denegación de servicios, crackers, código malicioso, robo de servicios, y espionaje industrial y externo. Asegurar la *confidencialida*d, *integrida*d, *autenticidad* y *disponibilidad* son los principales objetivos de toda política y práctica de seguridad informática.

Posibles ataques y amenazas a una red inalámbrica

- **Espionaje**: Este tipo de ataque consiste simplemente en observar el entorno donde se encuentra instalada la red inalámbrica. Sirve para recopilar información y se puede combinar con otros tipos de ataques.

- ***War-Chalking***: Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que "pasen por allí". Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

- ***War-driving*****:** Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como una *notebook* o un PDA. El método es realmente simple: el atacante pasea con el dispositivo móvil, y en el momento en que detecta la existencia de la red realiza un análisis de la misma.

-**Interceptar una señal:** El atacante intenta identificar el origen y el destino que posee la información. Es decir, la toma de posesión y el uso del ancho de banda de las WLAN privadas y de los puntos de acceso públicos para recopilar información sensible del sistema.

-**Escuchas e intercepción**: El programa monitoriza los datos y determina hacia donde van, de donde vienen y qué son, siempre que haya una tarjeta de red que actúa en "modo promiscuo". El modo promiscuo es un modo de operación en el que una computadora conectada a una red compartida captura todos los paquetes, incluyendo los paquetes destinados a otras computadoras.

-**Secuestro y Burla**: El atacante falsifica información, un identificador de usuario o una contraseña permitidos por el sistema atacado. Esto lo hace redefiniendo la dirección física o MAC de la tarjeta inalámbrica por una válida ("*hijacking*"). De esta manera, asocia una dirección IP válida del sistema atacado. La idea es secuestrar la comunicación entre dos sistemas suplantando a uno de ellos, para lo que es necesario estar situado en la ruta de comunicación.

Denegación de servicio (DoS) o ataques por inundación: La denegación de servicio sucede cuando un atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica. Impide a los usuarios legítimos de ésta, disponer de dichos servicios o recursos.

3.3.2 Mecanismos de seguridad

Identificador de Servicios Básicos (SSID, *Service Set Identifier*): Necesario para establecer una comunicación. El estándar para WLAN, permite dos formas de trabajar con el SSID: Descubrimiento Pasivo, donde el cliente recibe una trama (*beacom frame*) [2] con la información del SSID y donde el AP difunde constantemente unas tramas de información y el Descubrimiento Activo, donde el cliente tiene que conocer el SSID porque el AP no ofrece *beacom frame* [22]. Este SSID también debe conocerlo la tarjeta de red para poder asociarlo con el AP y así proceder con la transmisión y recepción de datos en la red.

Direccionamiento MAC o filtrado de direcciones MAC: Se utiliza para evitar que se conecten clientes no deseados. Muchos AP ofrecen opciones para crear listas blancas de equipos que se pueden conectar en función de la dirección MAC de los clientes. Para ello, en el AP, se añaden las direcciones de las máquinas que serán permitidas en la red.

Contraseñas no estáticas *(*OTP*, One Time Password)*: Contraseña de un solo uso. Esta contraseña tiene como objetivo, dificultar el acceso de usuarios no autorizados a recursos protegidos. La contraseña es utilizada solo una vez, y se genera una contraseña nueva para la próxima.

802.11x: Proporciona un mejor mecanismo en el control y seguridad de acceso. Es un estándar previo para el control de acceso a redes basado en puertos, este proceso, utiliza las características físicas de la infraestructura de las redes

---

[2] Tramas cortas transmitidas para proporcionar: reloj (sincronización de tiempos), parámetros de FH o DS, SSID, mapa de indicación de tráfico y **t**asas de transmisión soportadas

interconectadas para autenticar los dispositivos conectados a un puerto LAN. Permite el transporte de tramas de *Protocolo de Autenticación Extensible (EAP[3], Extensible Authentication Protocol)* de los usuarios sobre redes cableadas e inalámbricas. La utilización de este estándar, evita que se asocien usuarios no autorizados con cualquiera de los puntos de acceso de la red. En la arquitectura 802.1x además del cliente y el autenticador que suele ser el AP, existe un servidor de autenticación que puede ser un Servidor de *Servicio de Usuarios Telefónico de Autenticación Remota (RADIUS, Remote Authentication Dial-In User Service)*, que intercambiará el nombre y credencial de cada usuario. Es el sistema más capaz para la autorización y administración de cuentas de usuarios, auditorias y alarmas ya que permite la organización y el mantenimiento de los perfiles de usuarios en una base de datos central que puede ser administrada desde un servidor remoto en la red local cableada existente [23]. Para habilitar esta opción le asignamos al punto de acceso una IP y un puerto que debe ser conocido por el servidor *Radius*. El puerto por defecto es el 1812 y una contraseña de seguridad para el acceso al servidor *Radius* y por ultimo se habilita una cuenta en el servidor que se nombra *Radius account service*. El puerto por defecto que se usa es el 1813. Del lado del cliente es necesario también configurar la seguridad y los métodos de autenticación usados por *Windows XP* que incluye nombre de usuario, contraseñas y certificados.

Cifrado o Encriptación

Entre los mecanismos que utilizan las WLAN para la encriptación, se encuentra WEP, que utiliza una palabra clave para autenticarse en redes WEP cerradas y para cifrar los mensajes de la comunicación. Este protocolo es implementado sobre la capa MAC, sólo comprime y cifra los datos que se van a transmitir. Se basa en un esquema de cifrado simétrico en el que la misma clave y algoritmo se

---

[3] Existen múltiples variantes de EAP: EAP-LEAP (*Lightweight EAP*), EAP- TLS (*Transport Layer Security*), EAP-TTLS (*Tunneling Transport Layer Security*) y EAP-PEAP (*Protected EAP*)

utilizan, tanto para el cifrado de los datos, como para su descifrado. Permite crear llaves compartidas que tienen que ser conocidas por todas las estaciones que estén conectadas al mismo AP. Estas llaves pueden usar algoritmos de 40 y 128 bits .Las llaves de 40 dígitos pueden usar códigos ASCII de 5 caracteres desde la "A-Z" y "0-9" y hexadecimales de 10 dígitos en el rango de "A-F", "a-f" y "0-9" (e.j. 11AA22BB33).Las de 128 dígitos pueden usar códigos ASCII de hasta 13 dígitos y hexadecimales de hasta 26 dígitos. Este protocolo permite poner una llave compartida y generar hasta 4 palabras claves. [24].

Con el objetivo de realizar una encriptación más segura surge WPA. Está basado en el estándar IEEE 802.11i y usa una clave en constante rotación, cada paquete de información lleva una clave completamente diferente a los anteriores. WPA utiliza 802.1x y EAP (*Enterprise mode*) como base de su mecanismo de autentificación, haciendo uso de un servidor *RADIUS*. Existe un modo de trabajo denominado WPA- PSK (*Pre-Shared Key*, Llave Pre Compartida) que únicamente requiere una contraseña para acceder al punto de acceso para garantizar mayor seguridad y privacidad en la transmisión de los datos entre la estación y el punto de acceso. Usa una llave pre compartida que no requiere autentificación contra un servidor *RADIUS*. Igualmente admite caracteres desde a-z, A-Z, 0-9. La comunicación solo se establece cuando la llave pre compartida es igual a la del dispositivo inalámbrico al que se necesita conectar.

WPA (WI-FI *Protected Access*) realiza la encriptación mediante el Protocolo de Integridad de Clave Temporal *(TKIP, Temporal Key Integrity Protocol)* donde cada usuario tiene su propia clave de encriptación, puede ser establecida de modo que cambie periódicamente y la Codificación de Integridad del Mensaje *(MIC, Message Integrity Code)* para distribuir claves dinámicas temporales a los clientes y comprobar la integridad de las tramas recibidas.

En el año 2004 aparece WPA2, que es la segunda generación del WPA. Este proporciona encriptación con un fuerte algoritmo llamado Estándar de Encriptación Avanzada *(AES, Advanced Encriptation Standard)* y está contemplado también en el estándar IEEE 802.11i. Se trata de un algoritmo de cifrado de bloque con claves

de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Para asegurar la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP *(Counter-Mode/ Cipher Block Chaining / Message Authentication Code Protoco*l) en lugar de los códigos MIC .WPA2 incluye soporte no sólo para el modo BSS sino también para el modo IBSS (redes *ad-hoc*).

3.3.3 Autenticación y control de acceso

Configuración del punto de acceso inalámbrico con WPA.

Para la autenticación de clave previamente compartida WPA y el cifrado TKIP, debe configurar el punto de acceso inalámbrico con las siguientes opciones:

Nombre de la red inalámbrica (SSID).

Habilitar WPA con cifrado TKIP.

Habilitar la autenticación de clave previamente compartida WPA.

Escribir la clave previamente compartida WPA.

La clave WPA previamente compartida debe ser una secuencia aleatoria de caracteres de teclado (letras mayúsculas y minúsculas, números y signos de puntuación) de una longitud mínima de 20 caracteres o dígitos hexadecimales. En la figura 3.1 se aprecia como configurar la seguridad asociada a un AP.

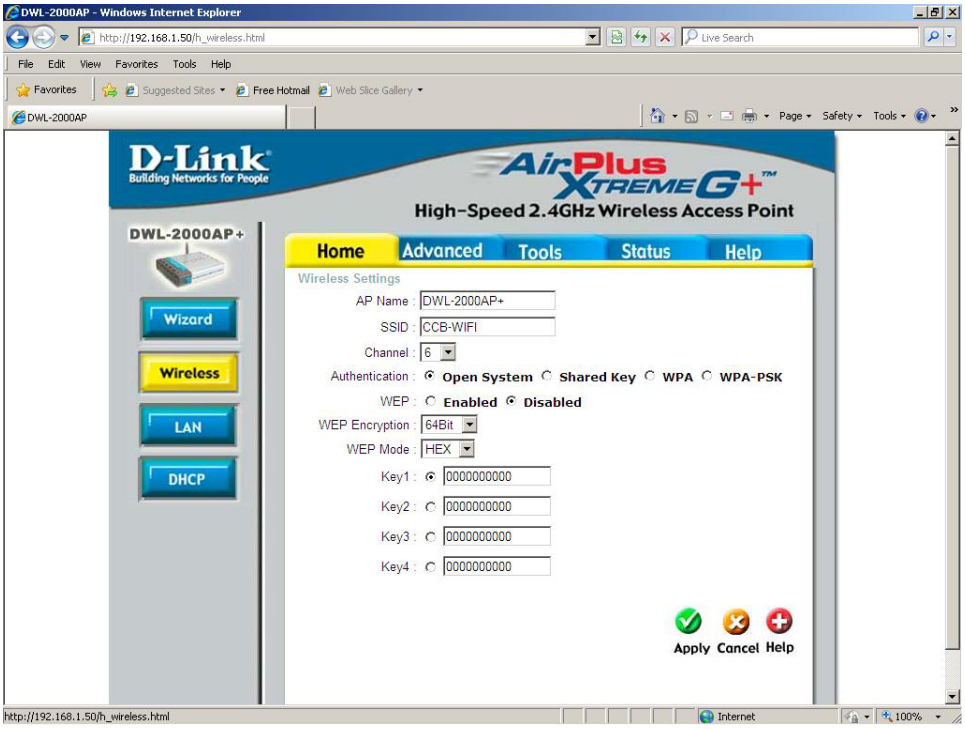


Figura 3.1 Ejemplo de configuración de la seguridad de un AP.

3.4 Requerimientos para el montaje y puesta en marcha de la red

Para el montaje y puesta en marcha de la red inalámbrica se necesita una vez localizados los lugares exactos donde colocar los AP, que existan facilidades de red eléctrica con su protección de tierra física, que exista disponibilidad de red cableada para su interconexión con la red principal, en este caso se dispone de cable par trenzado UTP 6. Por las características propias de los AP que se utilizan para esta red inalámbricas los mismos serán colocados en interiores preferiblemente climatizados pues su temperatura de operación es entre 0^{o}C y 55^{o}C, además de las mediciones realizadas y descriptas en el capitulo II tomamos que los AP se deben colocar a una altura de 2 metros, para lo cual se procede a anclarlos a la pared a esa altura.

3.5 Conclusiones

Para una red domestica o de pequeña empresa se debe usar como protocolo de autenticación *(RADIUS, Remote Authentication Dial-In User Service)* es el sistema

más capaz para la autorización y administración de cuentas de usuarios, auditorias y alarmas ya que permite la organización y el mantenimiento de los perfiles de usuarios en una base de datos central que puede ser administrada desde un servidor remoto en la red local cableada existente.

Asociado al protocolo de autenticación de usuarios se debe implementar como mecanismo de seguridad WAP, siempre que exista un controlador de dominio y esté implementado un servidor RADIUS en la red.

Conclusiones

CONCLUSIONES

1. Se realizó el diseño teórico de una red de área local inalámbrica para interconectar las áreas del Centro de Convenciones Bolívar con la red cableada del lugar.
2. Se configuró la red de área local inalámbrica para proporcionar un adecuado y eficiente medio de accesibilidad, autenticación y seguridad de redes para los usuarios de la misma.
3. Se corroboró que los equipos de tecnología inalámbrica, están diseñados para cumplir con determinados requerimientos; su selección está en dependencia de las necesidades del usuario y del lugar donde se va a utilizar.
4. Las redes de área local inalámbricas constituyen una alternativa a las redes cableadas y permiten la comunicación mediante ondas de radio.
5. Las velocidades alcanzadas por redes 802.11n constituyen un gran atractivo para los consumidores, sin embargo, la velocidad de una red inalámbrica la fija el usuario más lento, por lo que solo en algunos casos se podrá sacar ventaja de la velocidad.

Recomendaciones

RECOMENDACIONES

Con este trabajo se llega hasta del diseño de la red aunque se describe la manera en que puede ser configurado y se hacen estudios y pruebas de tráfico y ocupación del canal. Queda pendiente entonces el montaje oficial del equipamiento, la configuración y puesta en marcha del enlace tomando como base todo el estudio y las pruebas practicas que se hicieron con los equipos disponibles.

Se recomienda que este trabajo se realice de conjunto con personal técnico de la empresa proveedora del equipamiento y el departamento de informática del Centro de Convenciones Bolívar. Por lo que se proponen las siguientes recomendaciones:

1. Aplicar el diseño teórico de la red al montaje del equipamiento y las experiencias prácticas que se dan en los capítulos 2 y 3 para la configuración y rendimiento de la subred que se creará.
2. Utilizar las WLAN para lograr la redundancia de la red y en el caso que existan fallas, no se afecten los servicios.
3. Utilizar para el montaje de la red dispositivos de la norma IEEE 802.11 b/g ya que la red cableada es del tipo 100 Mbps (*Fast Ethernet).*

Referencias Bibliográficas

REFERENCIAS BIBLIOGRÁFICAS

[1] Walke, B.H. et al. (2006) *IEEE 802 Wireless Systems. Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence*. Editorial John Wiley & Sons, Ltd.

[2] Beltrán, D. (2009) "*Redes Inalámbricas de Área Local". Sistemas Inalámbricos*. Curso de Maestría en Telemática, Febrero 2009, Santa Clara, Facultad de Ingeniería Eléctrica, UCLV. Cuba.

[3] Ramos A, Herrera F. y D. Beltrán (2007) *Enlace inalámbrico en la red UCLV.* CIE2007, Santa Clara. Cuba.

[4] García, R. (2006) "*Políticas Regulatorias. Nuevas Tecnologías y Convergencia. Aspectos Regulatorios*". *Seminario de Difusión de las Telecomunicaciones*, miércoles 8 de noviembre del 2006. Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

[5] Ghetie, J. (2008) *Fixed-Mobile Wireless Networks Convergence. Technologies, Solutions, Services*. Editorial Cambridge University Press.

[6] Guizani, M. y H.H. Chen (2006) *Next Generation Wireless Systems and Networks*. Editorial John Wiley & Sons, Ltd.

[7] Flickenger, R. et al. (2007) *Redes Inalámbricas en los Países en Desarrollo*. Segunda Edición. Editorial Limehouse Book Sprint Team.

[8] Haykin, S. y M. Moher (2005) *Modern Wireless Communications*. Editorial Pearson Education, Inc. Prentice Hall.

[9] Gipson, J.D. (2002) *The Communications Handbook*. Segunda Edición. Editorial CRC Press.

[10] Mandal, A. (2008) *Mobile WiMAX: Pre-Handover Optimization Using Hybrid Base Station Selection Procedure*. Tesis de Maestría. Universidad de Canterbury.

[11] Guizani, M. y H.H. Chen (2006) *Next Generation Wireless Systems and Networks*. Editorial John Wiley & Sons, Ltd.

[12] Haykin, S. (2001) *Communication Systems*. Cuarta Edición. Editorial John Wiley and Sons, Inc.

[13] Määttänen, H. (2005) *"MIMO Principles"*. *Postgraduate Course in Radio Communications*, 2005. Communications Laboratory, Helsinki University of Technology.

[14] Singhai, S. K. (2001) *Understanding Wireless LAN Security*. ReefEdge Inc.

[15] Hernando, J. M. (1995) *Transmisión por radio,* 4ª Edición, Editorial Centro de Estudios Ramón Acres, S.A. ETSIT. España.

[16] Wang, X. y H. Vincent Poor, (2003) *Wireless Communication Systems: Advanced Techniques for Signal Reception*. Prentice Hall. EUA.

[17] Matos, J.; (2005) TV *Directa por satélite*. España.

[18] Ramos Pascual, F. (2005) "*Medidas de distorsión no lineal en dispositivos de radiofrecuencia (Parte I)"* en *Radiocomunicaciones y fibra óptica.* [En línea]. España, disponible en: http://www.radioptica.com/Radio/intermodulacion_I.asp?pag=2 [Accesado el día 4 de mayo de 2010].

[19] García Fernández, Néstor., (2005) *Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo*. Trabajo Doctoral. Universidad de Oviedo. [En línea]. España, disponible en: http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf [Accesado el día 4 de mayo de 2010].

[20] Earte, A. (2006). *Wireless Security handbook.* Boca Raton, FL, Taylor & Francis Group, LLC.

[21] Cors, I; Pernich, P. (2004). *Seguridad en redes wireless*.

[22] Alonso, Ch. (2006) "*¿Cómo proteger una red inalámbrica?*" en *PC-World*. [En línea]. España, disponible en: http://www.idg.es/pcworldtech/estructura/imprimir.asp?id=297748118&cat=art [Accesado el día 5 de mayo de 2010].

[23] Figueroa Domínguez, M. V., y D. Merinto Mateo., (2004) "*Soluciones de seguridad en redes inalámbricas*" en *Astic*. [En línea]. España, disponible en: www.astic.es/SiteCollectionDocuments/Astic/Documentos/Boletic/Boletic%2032/mono04.pdf [Accesado el día 4 de febrero de 2010].

[24] Caballé, X., (2005) "*Demostrado: el cifrado WEP no sirve para nada*" en *Hispasec sistemas*. [En línea]. Disponible en: http://www.hispasec.com/unaaldia/2398 [Accesado el día 7 de abril de 2010].

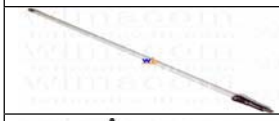
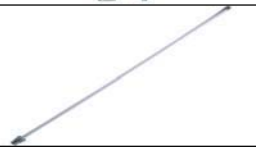
Anexos

ANEXOS

Anexo I Puntos de Acceso

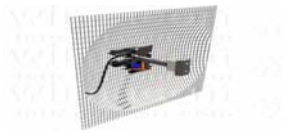
Producto	Descripción	Precio
	D-Link AirPlusXTREME G+ DWL-2000AP+ High-Speed 2.4GHz Wireless Access Point 54Mbps 802,11b/g	54,30 EUR
	Conceptronic [C54APM] Punto de Acceso Bridging Wireless 54Mbps 802,11g Conector Antena RP-SMA	39,95EUR
	D-Link [DI-524UP] Router Punto de Acceso con USB Print Server 54Mbps 802,11b/g 4 Ethernet con Conector Antena RP-SMA	55,90EUR
	Linksys [WAP54G-EU] Punto de Acceso Wireless 54Mbps 802,11g 2x Conector Antena RP-TNC	59,95EUR
	Linksys [WRT54GL-EU] Router Punto de Acceso Wireless 54Mbps 802.11g 4 Ethernet 2x Conector Antena RP-TNC linux	56,95EUR
	Ovislink [EVOW108AR] Router Punto de Acceso Wireless 108/54/11 Mbps + 1 Puerto WAN + 4 Puertos 10/100 Mbps. Chipset Athero	71,99EUR
	Senao [NOC-3220-EXT] Engenius Punto de Acceso Wireless 802,11b/g Exterior Punto Multipunto WDS Bridge Conector RP-SMA (400mW)	202,36EUR
	StraightCore [SC GWP-106VE] Punto de Acceso Wireless 802,11b/g Para Exterior con Antena Planar de 14dbi Incorporada + POE	119,95EUR
	Wifisafe [X-MINITAR-ABG] Punto de acceso Tribanda AP/bridge/cliente Minitar 802.11 a/b/g 54Mbps con 5 Ethernet conector RP-SMA	83,99EUR
	Wisacom [WISACOM 54G] Acces Point para exterior 802.11b/g Multi-funcional (AP/Bridge/Repeater/Cliente) antena panel interna	238,80EUR

Anexo II Antenas Omnidireccionales

Productos	Descripción	Precios
	[AO24-15DBEXNH] de 15dBi para 2,4GHz Exterior Con Conetor N Hembra	68,90EUR
	[AO24-5DBBMCMC] de 5dBi para 2,4GHz Base Magnética Conector MC	15,50EUR
	[AO24-7DBBMC-MMCX] de 7dBi para 2,4GHz Base Magnética Conector MMCX Desmontable.	23,95EUR
	CyberBajt [CYB-AO-10] de 10 dB para 2,4Ghz Exterior Conector N Hembra	39,95EUR
	Interline [INT-HOR-09-24-V] de 9 dB para 2,4Ghz Exterior Conector N Hembra	49,95EUR
	Interline [INT-HOR-12-24-V] de 12 dB para 2,4Ghz Exterior Conector N Hembra	69,25EUR
	Ovislink [WAE-120V] de 12dBi para 2,4GHz Exterior Con Conetor N Hembra	78,95EUR
	Ovislink [WAE-85] de 8,5dBi para 2,4GHz Exterior Con Conetor N Hembra	63,95EUR

Anexo III Antenas Parabólicas

Productos	Descripción	Precios
	Equinox [SA 2415F] Antena Parabólica Rejilla de 15dBi para 2,4GHz Exterior Con Conector Antena N Hembra	45,60EUR

	Equinox [SA 2424F] Antena Parabólica Rejilla de 24dBi para 2,4GHz Exterior Con Conector Antena N Hembra	68,40EUR
	Interline [INT-PAR-27-24-HV] Antena Parabólica de 27dBi para 2,4GHz Exterior Con Conector N Hembra	113,95EUR
	Stella Doradus [24 SD21] Antena Parabólica de Rejilla SD21 de 20,5dBi para 2,4GHz Exterior Conector N Macho	34,95EUR

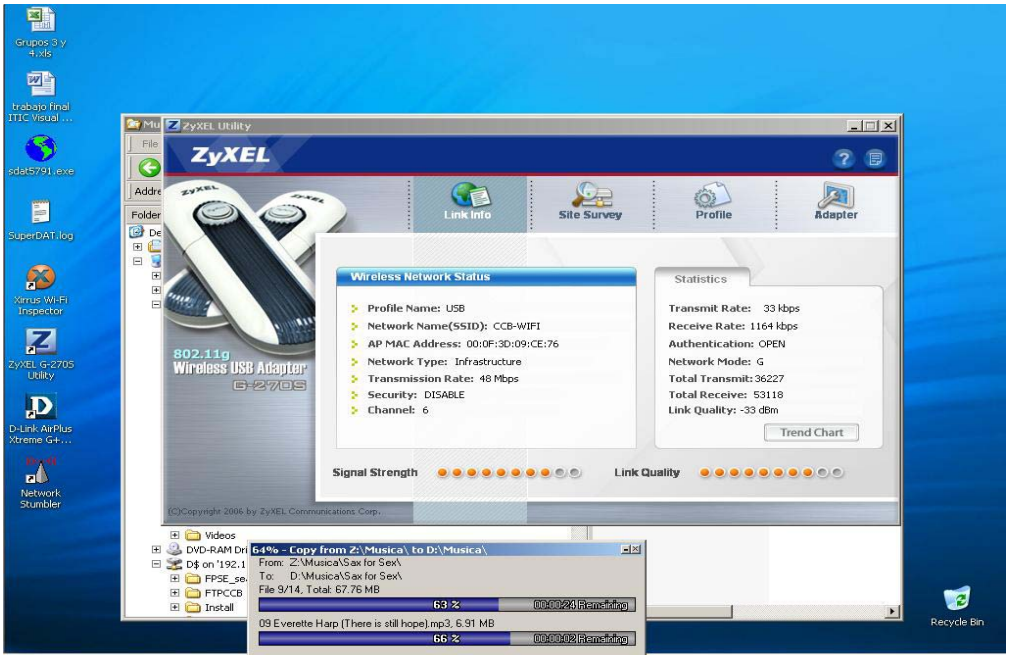
Anexo IV Antenas Panel (direccionales)

Producto	**Descripción**	**Precio**
	CyberBajt [CYB PAN 11-3M-NH] de 11,5dBi para 2,4GHz para Exterior Conector N Hembra 3 Metros de Pigatil	19,95EUR
	Interline [INT-PAN-14-24-HV] de 14dBi para 2,4GHz Exterior Con Conector N Hembra	24,95EUR
	Ovislink [WAE-180PM] de 18dBi para 2,4GHz para Exterior Con Conector N Hembra de Larga Distancia	86,95EUR

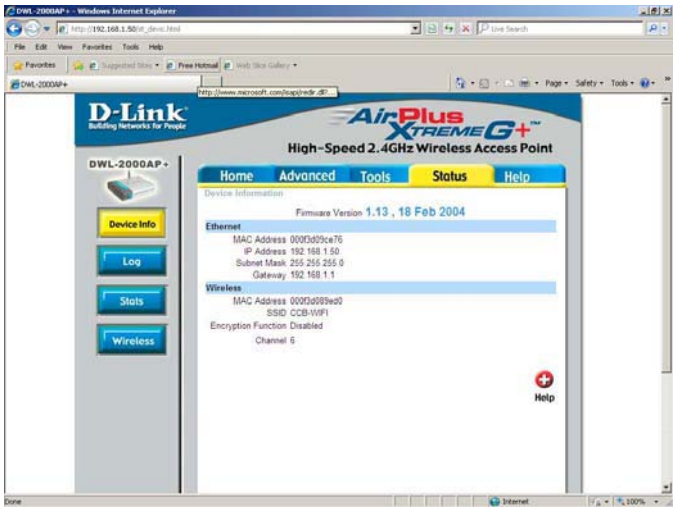
Anexo V Antenas Sectoriales

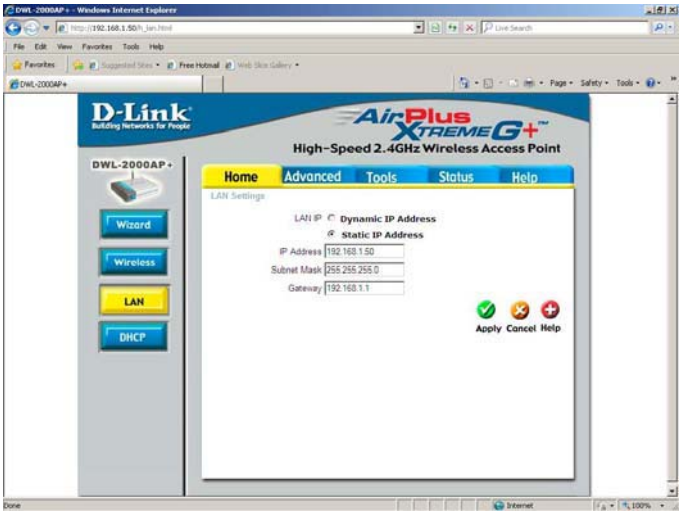
Producto	**Descripción**	**Precio**
	Interline [INT-SEC-15-24-V] de 15dBi 88º x 8º para 2,4Ghz Exterior Con Conector N Hembra	109,95EUR
	Interline [INT-SEC-17-24-V] de 17dBi para 2,4Ghz Exterior Con Conector N Hembra	114,95EUR

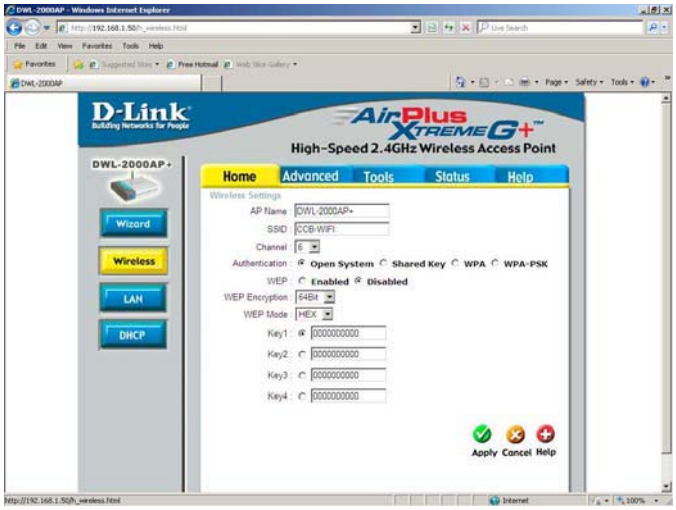
Anexo VI Características de la señal luego de colocar 3 AP.



Anexo VII Configuración de un AP.







Glosario

GLOSARIO

AP (*Access Point*) Punto de Acceso, dispositivo encargado de establecer la comunicación entre una estación en una WLAN con la red local correspondiente.

BSS (*Basic Service Set*) Grupo de Servicio Básico, conjunto de estaciones que compiten por acceder a un mismo AP conectado a un sistema de distribución.

CCK (*Complimentary Code Keying*) Conmutación de Códigos Complementarios.

CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) Acceso Múltiple por Detección de Portadora Evitando Colisión.

DSSS (*Direct Sequence Spread Spectrum*) Técnica de Espectro Extendido de Secuencia Directa.

EAP (*Extensible Authentication Protocol*) Protocolo de autenticación.

ESS (*Extended Service Set*) Grupo de Servicio Extendido.

ECIE (Empresa de Construcción y Mantenimiento de la Industria Eléctrica).

ETSI (*European Telecmomunication Standards Institute*) Instituto Europeo de Estándares de Telecomunicaciones.

FHSS (*Frequency Hopping Spread Spectrum*) Técnica de Espectro Extendido por Salto de Frecuencia.

HiperLAN (*High Performance Radio LAN*) Estándar inalámbrico europeo de alto desempeño en redes WLAN. Se le reconocen 4 tipos fundamentales: HiperLAN 1 y 2, HiperACCESS e HiperLINK, cada uno con características y aplicaciones específicas.

IBM (*International Business Machine*) Máquina de Negocios Internacional.

IBSS (*Independient Basic Service Set*) Grupo de Servicio Básico Independiente.

IEEE (*Institute of Electrical and Electronics Engineers*) Instituto de Ingenieros Eléctricos y Electrónicos.

IEEE 802 Comité de la IEEE organizado para crear los estándares de las Redes de Área Local. La IEEE 802.11 especifica las normas para las redes LAN inalámbricas.

IP (*Internet Protocol*) Protocolo de Internet.

ISM (*Industrial Scientific Medical*) Bandas de aplicaciones industriales, científicas y médicas.

ITU (*International Telecommunication Union*) Unión Internacional de Telecomunicaciones.

LAN (*Local Area Network*) Red de Área Local.

LDAP (Lightweight Directory Access Protocol) Protocolo de acceso al directorio de peso ligero

LOS (*Line-of-Sight*) Línea visual.

MAC (*Medium Access Control*) Control de Acceso al Medio.

MAN (*Metropolitan Area Network*) Red de Área Metropolitana.

MIC *(Message Integrity Control)* Control de Integridad del Mensaje.

MIMO (*Multiple Input Multiple Output)* Múltiple Entrada Múltiple Salida.

NIC (*Network Interface Card*) Tarjeta de Interfaz de Red.

NLOS (*Non-Line-of-Sight*) Fuera de la línea visual.

OFDM (*Orthogonal Frequency Division Multiplexing*) Multiplexación por División de Frecuencias Ortogonales.

OBE (Organización Básica Eléctrica)

OLOS (*Obstructed-Line-of-Sight*) Línea visual obstruida.

OSI (*Open system interconexion*) Sistemas de interconexión abiertos.

OTP *(One Time Password)* Contraseñas no Estáticas.

PAN (*Personal Area Network*) Red de Área Personal.

PCF (*Point Coordinate Function*) Función de Coordinación Puntual.

PDU (*Protocol Data Unit*) Unidades de datos de protocolo.

PHY (*Physic*) Nivel Físico.

PLCP (Physical Layer Convergenve Protocol) Protocolo de convergencia de la capa física)

PSK *(Pre Shared Key)* Llave PreCompartida.

QAM (*Quadrature Amplitud Modulation*) Modulación de Amplitud en Cuadratura.

QoS (*Quality os Service*) Calidad de Servicio.

QPSK *(Quadrature Phase Phase Shift Keying)* Modulación Cuaternaria por Desplazamiento de Fase.

RADIUS (*Remote Aunthentication Dial In User Service*) Servicio de Usuario de Acceso Telefónico de Autenticación Remota.

SHF (*Super High Frequency*) Súper alta frecuencia.

SNMP *(Signaling Network Main Protocol)* Protocolo Principal de Señalización de Red.

SIDD (*Service Set Identifier*) Identificador del Grupo de Servicio.

SPT (Sistema de puesta a tierra)

STA (Estación cliente).

TCP (*Transport ControlProtocol*) Protocolo de Control de Transporte.

TIA (Telecommunication Industry Association) Asociación de Industrias de Telecomunicaciones)

TKIP (*Temporal Key Integrity Protocol*) Protocolo de integridad de clave temporal.

TPC (*Transmitier Power Control*) Control de Potencia del Transmisor.

UHF (*Ultra High Frequency*) Banda de frecuencias ultra altas entre 300 y 3000 MHz.

UDP *(User Datagrama Protocol)* Protocolo de Datagrama de Usuario.

UNII *(Unlicenced National Information Infrastructure)* Infraestructura de Información Nacional Sin Licencia.

VHF (Very High Frecuency) Bandas de frecuencias muy altas.

VoIP (*Voice over IP*) Voz sobre IP.

WAN (*Wide Area Network*) Red de Área Extendida.

WECA (*Wireless Ethernet Compatibility Alliance*) Alianza de Compatibilidad en Ethernet Inalámbrica.

WEP (*Wired Equivalent Privacy*) Equivalente a Privacidad Cableada, protocolo de seguridad en redes WLAN.

WDS (*Wireless Distribution System*) Sistema de Distribución Inalámbrica.

Wi-Fi (*Wireless Fidelity*) Fidelidad Inalámbrica certificación a los productos de redes WLAN.

Wi-Fi 5 (*Wireless Fidelity 5*) Certificación Wi-Fi para la tecnología dentro de la banda de los 5 Ghz.

WLAN (*Wireless Local Area Network*) Red de Área Local Inalámbrica.

WMAN *(Wireless Metroplitan Area Network)* Red de Área Metropolitana Inalámbrica.

WPA (*Wi-Fi Protected Access*) Acceso Protegido Wi-Fi, protocolo de seguridad altamente confiable.

WPA2 *(Wi-Fi Access Protected 2)* Acceso Protegido Wi-Fi 2.

WPAN *(Wireless Personal Area Network)* Red de Área Personal Inalámbrica.

WWAN *(Wireless Wide Area Network)* Red de Área Extendida Inalámbrica.