



Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

“Diseño de una red de área local inalámbrica”

Tesis Presentada en Opción al Título Académico de

Master en Telemática

Maestría de Telemática

Autora: Ing. Arelys Ramos Fleites

Tutores: Dr. Francisco Herrera Fernández

Mcs. David Beltrán Casanova

Santa Clara, Cuba

2007

“Año 49 de la Revolución”



Departamento de Telecomunicaciones y Electrónica



Tesis de Maestría

“Diseño de una Red de Área Local Inalámbrica”

Autora: Ing. Arelys Ramos Fleites.

Tutores: DR. Francisco Herrera Fernández.
Profesor Titular del Departamento de Automática
Facultad de Ingeniería Eléctrica.
e-mail: herrera@uclv.edu.cu

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

Santa Clara

Curso 2007-2008

“Año 49 de la Revolución”



Hago constar que el presente trabajo en Opción al Título Académico de Master en Telemática fue realizada 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 de la Autora

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

Firma de la Autora

**Firma del Jefe de
Departamento donde se
defiende el trabajo**

**Firma del Responsable de
Información Científico-Técnica**

TAREAS TÉCNICAS

Las tareas a realizar en este trabajo son:

- Revisión y estudio bibliográfico sobre la actualidad de las redes inalámbricas en el mundo y la radio propagación.
- Revisión del equipamiento más usado en el mundo para instalar redes inalámbricas particularizando el que se comercializa en Cuba.
- Visita a instituciones y organizaciones donde hay soluciones inalámbricas, las cuales sirven como casos de estudio.
- Definir y caracterizar el tipo de tecnología a usar para lograr la calidad del enlace
- Confección del proyecto de diseño del radio enlace para unir las áreas de Eléctrica-Jardín Botánico.
- Definir proyecto del sistema de tierra en el área del Jardín Botánico para garantizar la durabilidad de los equipos de radio y la red contra las descargas eléctricas.
- Definición del sistema de administración del enlace.
- Hacer estudios del tráfico para enlaces que tengan las mismas características que el diseñado en este trabajo.

Firma de la Autora

Firma del Tutor

RESUMEN

Se realizó el diseño de una red inalámbrica de área local, con el objetivo de enlazar sitios que están fuera de una red, para dar solución a los problemas de interconexión a lugares de difícil instalación de una infraestructura cableada. El objeto de aplicación de los resultados de esta tesis lo constituye el enlace inalámbrico entre el Jardín Botánico y la Facultad de Ingeniería Eléctrica de la UCLV, logrando de esta forma adicionar una nueva área a la red de computadoras de este centro de estudios. Se tuvo en cuenta para el diseño la distancia entre los puntos a enlazar, la altura a la que deben estar las antenas, 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 diferentes documentos y se tomó como caso de estudio un enlace con las mismas características de equipamiento y tipo de enlace que existe en la Empresa de Construcción y Mantenimiento de la Industria Eléctrica (ECIE) de Santa Clara, básicamente en lo relacionado con la administración y el tráfico en el enlace. Finalmente se presenta el correspondiente proyecto técnico del sistema de aterramiento contra descargas eléctricas.

TABLA DE CONTENIDOS

TAREAS TÉCNICAS	IV
RESUMEN	V
INTRODUCCIÓN	1
Organización del informe	3
Capítulo I. Aspectos teóricos sobre redes WLAN y Radio propagación.....	4
1.1 Ventajas y desventajas de las redes de área local inalámbricas.....	4
1.1.1 Componentes de una red Wireless.....	5
1.2 Topología de redes WLAN.....	7
1.2.1 Topología ad-hoc	7
1.2.2 Topología infraestructura.....	8
1.2.3 Enlace entre varias LAN.....	9
1.3 Estándares Inalámbricos	9
1.3.1 Estándares IEEE	9
1.4 Tecnologías en WLAN	13
1.4.1 Espectro extendido (SS).....	13
1.4.1.1 Espectro Extendido por Secuencia Directa (DSSS)	13
1.4.1.2 Espectro extendido por salto de frecuencia (FHSS)	14
1.4.2 Otras tecnologías de radio de redes WLAN	14
1.4.2.1 Multiplexación por División de Frecuencias Ortogonales (OFDM)	14
1.4.2.2 Conmutación de Códigos Complementarios (CCK)	15
1.4.2.3 Conmutación de Códigos Complementarios/Multiplexación por División de Frecuencias Ortogonales (CCK/OFDM)	16
1.4.2.4 Codificación Convolutiva de Paquetes Binarios (PBCC).....	16
1.5 Bandas de Frecuencia	16

TABLA DE CONTENIDOS

1.6	Acceso al medio	17
1.6.1	Función de Coordinación Distribuida	18
1.7	Radiopropagación	19
1.7.1.	Conceptos.....	19
1.8	Mecanismos de propagación.....	21
1.8.1	Reflexión, Refracción y Absorción	22
1.8.2	Interferencia, ruido y distorsión.....	22
1.9	Análisis de las características de un radioenlace.	23
1.10	Tipos de antenas.....	24
1.10.1	Antenas Direccionales	24
1.10.2	Antenas Omnidireccionales	25
1.10.3	Antenas Sectoriales.....	26
1.11	Sensibilidad del receptor.....	26
1.11.1	Relación señal a ruido.....	26
1.11.2	Margen	26
1.12	Seguridad en redes WLAN	27
Capítulo II.	DISEÑO DEL ENLACE.....	33
2.1	Situación de la red UCLV.....	33
2.1.1	Análisis del entorno para enlazar la red con infraestructura cableada.....	35
2.1.2	Enlace inalámbrico	36
2.2	Diseño del enlace inalámbrico	36
2.2.1	Demostración de tierra plana	36
2.2.2	Distancia entre los puntos.	37
2.2.3	Altura de los Equipos.....	40

TABLA DE CONTENIDOS

2.2.4 Determinación de la primera zona de Fresnel	40
2.3 Oferta del equipamiento.....	41
Mercado Mundial.....	42
Oferta en Cuba	42
2.4 Selección del equipamiento	43
2.5 Características del K-BEST	44
Series BL 3 000-3010, BL3200	44
Datos del K-BEST BL-3201 802.11 b/g Outdoor radio	45
2.6 Análisis económico.....	47
2.7 Conclusiones.....	48
Capítulo III Consideraciones técnicas generales para la puesta en marcha del enlace.....	49
3.1 Sistema de tierra del Jardín Botánico.	49
3.1.2 Proyecto de diseño.....	49
3.2 Utilitario de administración para el KBEST	52
3.3 Monitoreo y Gestión del Enlace.	67
3.5 Soluciones alternativas de respaldo ante situaciones que comprometen la continuidad de los servicios de la red.	69
CONCLUSIONES	71
RECOMENDACIONES.....	72
REFERENCIAS BIBLIOGRÁFICAS	73
ANEXOS	78
GLOSARIO	88

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, Bluetooth (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 Commission)*, 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, Cayería Norte de Villa Clara, Radio Cuba, Etecsa, Copextel, Movitel, Cubalse, Sepsa, ECIE y con este trabajo comienza la Universidad Central “Marta Abreu” de Las Villas (UCLV) a introducir este nuevo tipo de tecnología y hacerla extensiva a la mayor parte del campus universitario.

Este trabajo surge porque existen áreas dentro de la universidad que no se pueden unir a la estructura central de la red, conocida comúnmente como *backbone*, porque las condiciones geográficas del terreno y en algunos casos la lejanía del área central, no lo

permiten y están actualmente privados de todos los servicios que brinda la red UCLV, constituye esto sin dudas un problema técnico al estar alejados de todo el proceso de informatización en que esta inmerso el país, incluyendo todas sus universidades. Además este proyecto constituye un punto de partida en la aplicación de enlaces inalámbricos en la Universidad Central.

Particularmente en la UCLV, se justifica el proyecto, ya que el campus universitario es muy extenso, y hay lugares que por las condiciones geográficas del terreno, es imposible llegar con el enlace por fibra óptica. De ahí la necesidad de buscar otras variantes en la instalación de las redes de comunicaciones, para lograr llevar a todas las áreas universitarias los servicios con que cuenta la red y que hoy están totalmente incomunicadas o en la mayoría de los casos usan, en sólo una máquina, una línea telefónica conmutada, para lograr al menos el servicio de correo electrónico.

Con el diseño que propone este trabajo se logrará enlazar de manera inalámbrica a la red UCLV el Centro de Investigación ubicado dentro del Jardín Botánico, que tiene determinado grado de complejidad debido a las características geográficas de la zona. La solución a los anteriores problemas contribuirá a elevar el nivel científico técnico del personal que allí labora y al desarrollo tecnológico de la universidad, 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:

Diseñar una red inalámbrica en la Universidad para enlazar las áreas que hoy están fuera de la red, en específico el Jardín Botánico, y de esta manera contribuir al completamiento de la red de computadoras de la UCLV.

Objetivos específicos:

- Un estudio sobre la definición de redes inalámbricas y sus diferentes estándares y características, incluyendo lo relacionado con la protección eléctrica.
- Tener la concepción del diseño teórico de un enlace inalámbrico.

- Un estudio sobre el equipamiento que se comercializa en el mundo para instalar redes inalámbricas y obtener definiciones, según las condiciones cubanas y cumpliendo los requerimientos técnicos, que proporcionen un enlace estable y con velocidades aceptables de transferencia de los datos.
- Obtener un campo de pruebas experimentales que permita estudiar otras alternativas de diseño de este tipo de redes.

Entre los principales resultados alcanzados en este trabajo se tienen:

- Diseño completo de un enlace inalámbrico punto a punto, que soluciona el enlace entre el Jardín Botánico y la Facultad de Ingeniería Eléctrica de la UCLV.
- Una metodología que sirva de guía para diseño del tipo de red WLAN trabajado en esta tesis.

Organización del informe

En el capítulo uno, se realiza un estudio de las redes inalámbricas de área local, las ventajas que presenta frente a las estructuras cableadas, los componentes que la integran, las distintas topologías que pueden ser configuradas, los estándares, la seguridad y el acceso al medio. Se definen algunos conceptos relacionados con la radio propagación entre ellos el cálculo de la zona de Fresnel, las definiciones de reflexión, difracción, interferencia y ruido, tipos de antenas entre otros, que ayudan a entender el funcionamiento completo de un enlace de radio y que proporcionan actualidad de las redes inalámbricas en el mundo.

En el capítulo dos, se realiza un análisis de la red UCLV y se exponen las deficiencias de la misma, se analizan las alternativas para la interconexión del Centro de Investigación del Jardín Botánico, se estudian las ofertas del mercado mundial y nacional para la obtención de los equipos del enlace y se realiza el diseño del enlace inalámbrico.

El capítulo tres se refiere a las características técnicas correspondientes a la puesta en marcha del enlace analizando el sistema de puesta a tierra, detalles administrativos para la configuración del equipo de radio a utilizar, haciendo particular énfasis en el estudio de tráfico y estabilidad del enlace.

Capítulo I. Aspectos teóricos sobre redes WLAN y Radio propagación.

Las Redes de Área Local Inalámbricas, conocidas por sus siglas WLAN o por Wi-Fi¹, es un sistema flexible de transmisión de datos, que utiliza como medio de transmisión el aire. Este sistema está implementado como una extensión o una alternativa de una red LAN cableada dentro de un edificio o de un campus. Están diseñadas, para proveer acceso a redes de diferentes localizaciones entre dispositivos de conmutación y como su medio de propagación es el aire se hace necesario en esta primera parte del trabajo abordar algunas ideas teóricas acerca de la radiopropagación de las ondas a través de los medios reales, analizando las soluciones compatibles con las condiciones de contorno que el medio impone usando las ecuaciones de Maxwell como base matemática para diseñar cualquier enlace inalámbrico, incluyendo elementos principales como la potencia del transmisor, la sensibilidad del receptor y las pérdidas en la transmisión. Se abordan también otros términos que caracterizan a un enlace de radio importantes para su comprensión.

1.1 Ventajas y desventajas de las redes de área local inalámbricas

En los últimos años, las WLAN han ido ganando gran popularidad, la cual se incrementa según aumentan sus prestaciones, se originan nuevas aplicaciones y disminuyen los costos de infraestructura. Las WLAN, permiten a sus usuarios acceder a información y recursos en tiempo real, sin necesidad de estar físicamente conectados a un determinado lugar. Un usuario dentro de una red inalámbrica, puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive, sobre áreas metropolitanas.

Estas redes tienen una serie de ventajas sobre una red fija, convirtiéndolas así, en una alternativa viable para dar solución a los problemas de interconexión de redes. Una de las ventajas es la movilidad, pues las redes inalámbricas posibilitan que los usuarios de una LAN, tengan acceso a la información en tiempo real, en cualquier lugar en el que están

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

desplegadas. Otra de las mejoras que presentan las WLAN, son la simplicidad y rapidez en la instalación, eliminando la necesidad de utilizar cables. Además proporcionan flexibilidad en la instalación, permitiendo a la red llegar a puntos donde el acceso es difícil para una LAN cableada. A lo anterior se suma el costo total de la inversión a largo plazo en toda la instalación de una WLAN es menor que en una red LAN cableada. Estos sistemas son más escalables en comparación con las redes de cable, porque se pueden configurar en diversas topologías para cumplir con las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones, son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red (DLINK Latinoamérica, 2004).

Otra de las ventajas las redes WLAN, es la movilidad, que es la posibilidad que tiene un usuario de moverse de un punto de acceso a otro dentro de la misma tecnología, es decir, puntos de acceso bajo el mismo estándar. (Novakovik, 2004). La Estética es también una de las ventajas de las redes Inalámbricas pues no usan estructuras cableadas que afean los interiores de edificios. La provisionalidad: si se va a instalar una red provisional esta es la mejor opción, por ejemplo en ferias, oficinas temporales o crecimientos urgentes de una red ya establecida y la robustez pues en ciertos entornos como fábricas con elevada humedad, agentes químicos agresivos, calor, etc. las instalaciones cableadas pueden sufrir una rápida degradación o ser inviables. Pero no todo son ventajas, hay una serie de parámetros en los que las redes cableadas ofrecen mayores prestaciones que las inalámbricas. La velocidad binaria es mucho mayor, obteniéndose velocidades máximas del orden de los Gbits, frente a 54 Mbps en una WLAN 802.11g compartidos entre varios usuarios. (Proakis, 2001)

1.1.1 Componentes de una red Wireless

Una estación inalámbrica, es una Computadora Personal (PC, Personal Computer) o una Laptop con una Tarjeta de Red Inalámbrica (NIC, Network Interface Card) con una antena que permite el intercambio de información. Esta tarjeta realiza las funciones de las tarjetas de red ethernet, adaptando las tramas ethernet que genera el PC, a las tramas del estándar inalámbrico y viceversa.

Puntos de Acceso (Access Point)

Este dispositivo nos permite conectar la red cableada a los clientes de la red inalámbrica; su función es convertir los datos que llegan por la interface UTP a señales de radio y viceversa en las instalaciones con AP internos y externos de corto alcance (en los internos la distancia máxima es de 40m a la redonda). Los puntos de acceso suelen disponer de dos antenas, una interfaz LAN RJ-45 10/100 Mbps para conectividad WAN y, en la mayoría de los casos, un puerto de consola para su configuración inicial. Generalmente también disponen de varias entradas de red LAN 10/100 al tener integrado un hub o un switch. Ver Anexo I. Los AP, pueden enlazarse de tres formas: punto a punto, punto a multipunto y redes malladas. El enlace punto a punto, une dos redes LAN a través del modo puente entre dos redes finales, el enlace punto a multipunto, conecta múltiples redes alambradas con el empleo del modo puente multipunto, y las redes malladas están formadas por APs conectados punto a punto, para que queden enlazados en forma de malla (Leyva, 2005: 13).

Tarjetas cliente

Este dispositivo permite conectar las computadoras clientes móviles a la red inalámbrica. Contiene integrada la parte de radio y el procesamiento de las señales a bits de datos.

Puentes (bridge)

Este dispositivo nos permite conectar lugares remotos a larga distancia con alcance máximo de 40 KM. En él se encuentra el transmisor de radio y el procesamiento de las señales a bits de datos.

Puentes de grupos de trabajo (Workgroup_Bridge)

Este dispositivo nos permite conectar rápidamente a un grupo de 8 computadoras conectadas por cable a un puente de grupo de trabajo mediante un enlace inalámbrico con un punto de acceso, facilitándonos la conectividad al *backbone* de la red LAN.

Pasarela *Wireless*

La función de una pasarela es gestionar de forma centralizada y homogénea una política de acceso, autenticación (Radius, Kerberos, certificados digitales, LDAP), cifrado y Calidad de Servicio, aplicando esta política a múltiples puntos de acceso muchas veces incompatibles entre sí. Es el que se encarga de la interoperabilidad entre puntos de acceso,

para que se puedan comunicar los AP de varias tecnologías de forma transparente, un punto de acceso puede ser una pasarela para comunicar a los demás.

Conmutadores inalámbricos

Al igual que en las redes LAN, también existen conmutadores de red para inalámbricos, que monitorizan las ondas de radio midiendo el rendimiento en tiempo real y reajustando las potencias de emisión para equilibrar la carga y evitar puntos ciegos. Incluso el software que incluyen permite importar los planos del edificio y situar los puntos de acceso en base a los cálculos de propagación por la base de datos de materiales, situando visualmente los accesos no autorizados mediante triangulación de los puntos de acceso.

Antenas

Este dispositivo nos permite transmitir y recibir las señales de radio y las envían a los puntos de acceso y los puentes para transformarlas en bits de datos. Dependiendo del alcance es la antena a utilizar.

Servidores de control de acceso

Funcionan como un sistema servidor centralizado y pueden controlar la autenticación, autorización y contabilidad (AAA) de los usuarios que acceden a los recursos corporativos a través de la red.

1.2 Topología de redes WLAN

La utilización de una red WLAN, depende de las necesidades de los consumidores y de las condiciones existente en el lugar. Las redes inalámbricas, se construyen utilizando dos topologías básicas. Estas topologías se pueden clasificar de distintas formas: administradas y no administradas, *hosted* y *peer-to-peer*, infraestructura y ad-hoc (Fout, Barkley y Lee, 2007).

1.2.1 Topología ad-hoc

Una topología ad-hoc está formada por los dispositivos inalámbricos mismos, equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas, sin punto de acceso (Fig. 1.1) y son muy sencillas de implementar. Tienen integradas mecanismos de

usuario y de seguridad y típicamente no requieren de administración. Cada estación, mantiene una lista de usuarios de grupo y contraseña de grupo.

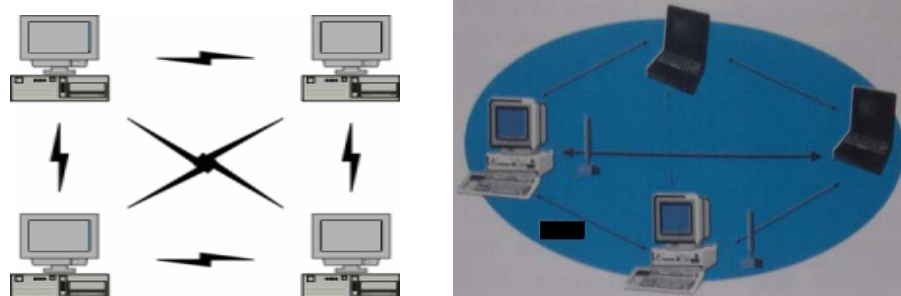


Figura 1.1. Ejemplos de topología Ad-hoc.

Ad-hoc es una configuración muy flexible, que no requiere un número elevado de terminales. (Calderón y Quintero, 2004).

1.2.2 Topología infraestructura

Esta topología, amplía una red cableada existente a dispositivos inalámbricos, a través, de un punto de acceso, actuando como controlador central para la red inalámbrica (Fig. 1.2). La infraestructura utiliza el concepto de celda. Una celda, podría entenderse, como el área en la que una señal radioeléctrica es efectiva. A pesar, que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión, es posible combinar celdas para cubrir de forma casi total un área más extensa. Un único punto de acceso puede soportar un pequeño grupo de usuarios. Esta topología aumenta el alcance de la red y permite la movilidad (García Fernández, 2005).

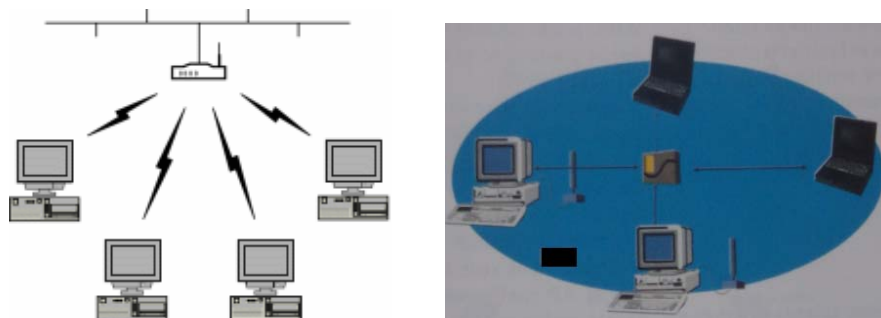


Figura 1.2. Ejemplos de Topología Infraestructura.

1.2.3 Enlace entre varias LAN

Esta configuración, se utiliza cuando se necesitan conectar dos o más redes de área local que están separadas, ya sea en edificios o instituciones, las cuales no se puedan unir por la vía cableada. Para ello es necesario el uso de antenas direccionales u omnidireccionales, las cuales tienen el objetivo de enlazar las redes de área local situadas geográficamente en sitios distintos.

1.3 Estándares Inalámbricos

Las redes WLAN cumplen con los estándares genéricos aplicables al mundo de las LAN cableadas (IEEE 802.3 o estándares equivalentes) pero necesitan una normativa específica adicional, que defina el uso y acceso de los recursos radioeléctricos. Varios organismos internacionales han desarrollado una amplia actividad en la estandarización de normativas de WLAN y han generado un gran número de estándares. Entre ellos podemos citar el IEEE que ha realizado una serie de estándares 802.11 y sus variantes; y en Europa el *Instituto de Estándares de Telecomunicaciones Europeo (ETSI, European Telecommunication Standard Institute)* que con sus actividades en *HiperLAN-BRAN (Broadband Radio Access Networks)* ha desarrollado estándares como Hiperlan tipo 1 y tipo 2, así como Hiperacces e Hiperlink. De esta manera se pueden diferenciar entre dos tipos de redes WLAN, las procedentes de IEEE y de ETSI.

1.3.1 Estándares IEEE

Como todos los estándares IEEE 802, el IEEE 802.11 centra su funcionamiento en las dos capas inferiores del modelo de referencia de *Interconexión de Sistemas Abiertos (OSI, Open System Interconnection)*: el *Nivel Físico (PHY, PhysicLayer)* y el *Nivel de Enlace de Datos (DLL, Data Link Layer)*, este último se subdivide en la capa de *Control de Acceso al Medio (MAC, Medium Access Control)* y *Control del Enlace de Datos (DLC, Data Link Layer)*, estas capas regulan la conexión vía radio.

La norma IEEE 802.11, se divide en estándares desarrollados por grupos de trabajo independientes, los cuales se identifican por medio de letras agregadas tras la última cifra. Cada vez que surge la necesidad de nuevas técnicas para solucionar un determinado

problema, el IEEE crea un nuevo grupo de trabajo incluido en el 802.11 e identificado por una nueva letra. (Luther, 2005).

- **IEEE 802.11 Legacy:** La versión original del estándar IEEE 802.11 fue publicada en 1997, especifica dos velocidades de transmisión teóricas de 1 y 2 Mbps que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. La señal IR sigue siendo parte del estándar, pero no hay implementaciones disponibles. El estándar original también define el protocolo de *Múltiple Acceso por Detección de Portadora / Evitando Colisiones (CSMA/CA, Carrier Sense Multiple Acces/Colission Avoidance)* como método de acceso y utiliza como técnicas de RF *Espectro Extendido por Salto de Frecuencia (FHSS, Frequency Hopping Spread Spectrum)* y *Espectro Extendido de Secuencia Directa (DSSS, Direct Sequence Spread Spectrum)*.

- **IEEE 802.11a:** Se aprobó en 1999 por el IEEE y en el año 2001 hizo su aparición en el mercado. El estándar IEEE 802.11a, también conocido como Wi-Fi , utiliza el mismo juego de protocolos de base que el estándar original y opera en la banda de 5 Ghz. Utiliza *Multiplexación por División de Frecuencias Ortogonales (OFDM, Orthogonal Frequency Division Multiplexing)* como tecnología de radio. Esta norma tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar IEEE 802.11b, sólo si se dispone de equipos que implementen ambos estándares. El alcance del sistema es pequeño en entornos cerrados, lo que implica tener que montar más AP. Algunos fabricantes ofrecen híbridos 802.11a/b, aunque estos productos lo que tienen realmente son las dos extensiones implementadas. (Geier, 2002)

- **IEEE 802.11b:** Este define los niveles físico y de acceso al medio. Es una extensión del 802.11 para WLAN empresariales. Ratificado en 1999. Utiliza como técnica de radio DSSS y *Conmutación de Códigos Convolutionales (CCK, Complementary Code Keying)*. Tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el método de acceso CSMA/CA. El estándar IEEE 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión de este estándar es de aproximadamente 5.9 Mbps sobre *Protocolo de Control de Transporte (TCP, Transport Control Protocol)* y 7.1 Mbps sobre *Protocolo de Datagrama de Usuario (UDP, User Datagrama Protocol)*. Las velocidades de datos son

de 11 Mbps, 5.5 Mbps, 2 Mbps y 1 Mbps. Ofrece una mejor penetración a través de las paredes y otros obstáculos, al igual que mayor distancia de operación en la oficina, en el hogar y en otros entornos encerrados.

- **IEEE 802.11c:** Especifica métodos para la conmutación inalámbrica, o lo que es lo mismo, métodos para conectar diferentes tipos de redes mediante redes inalámbricas (Luther, 2005).

- **IEEE 802.11d:** Es un complemento al nivel MAC en la familia IEEE 802.11, permitiendo así, el uso a escala mundial de este estándar en las redes WLAN. Se refiere a las diferencias regionales en tecnologías, relacionadas con el número y disponibilidad de canales en las distintas regiones del mundo y los niveles de potencia aceptables para los dispositivos de los usuarios.

- **IEEE 802.11e:** Fue publicado por el IEEE en noviembre de 2005. Su objetivo es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de *Calidad de Servicio (QoS, Quality of Service)*. Es un sistema eficiente de gestión de la energía de especial utilidad en teléfonos VoIP portátiles y otros dispositivos que funcionan con baterías (Fernández, 2007).

- **IEEE 802.11f:** Especifica un *Protocolo Entre Puntos de Acceso (IAPP, Inter-Access Point Protocol)* para la comunicación entre estos, independientemente de los proveedores y la marca de los productos..

- **IEEE 802.11g:** Se ratificó en junio de 2003. Este utiliza la banda de 2.4 GHz al igual que el estándar IEEE 802.11b pero opera a una velocidad teórica máxima de 54 Mbps. Utiliza las tecnologías de radio: DSSS y OFDM. Es compatible con el estándar IEEE 802.11b y utiliza las mismas frecuencias; sin embargo, en redes bajo este estándar, la presencia de nodos bajo el estándar IEEE 802.11b, reduce significativamente la velocidad de transmisión.

- **IEEE 802.11h:** Está destinado a resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélites en la banda de los 5 GHz.

- **IEEE 802.11i:** Estándar que se encarga de la seguridad mediante la encriptación avanzada y procedimientos de autenticación, según los requerimientos de alta privacidad

que sean solicitados. Es equivalente al protocolo *Acceso Protegido Wi-Fi 2 (WPA2, Wi-Fi Protected Access)* y es aplicable a los estándares IEEE 802.11a, IEEE 802.11b e IEEE 802.11g. Proporciona una alternativa a la *Privacidad Equivalente Cableada (WEP, Wireless Equivalent Privacy)* con nuevos métodos de encriptación y procedimientos de autenticación. Una parte clave de 802.11i la constituye IEEE 802.1x que explicaremos mas adelante.

- **IEEE 802.11j:** Está destinada a la interoperatividad entre el estándar IEEE 802.11a e HiperLAN.

Existen otros estándares en evolución que completan la norma. (Fernández G. E. 2007)

Resumen Estándares IEEE 802.11

802.11a - Transmisión de Datos en la Banda de 5GHz

802.11b - Transmisión de Datos en la Banda de 2.4GHz .Hasta 11 mbps.

802.11e - QoS - Calidad de Servicio

802.11g - Transmisión de Datos Adicional Banda 2.4 GHz. Hasta 54mbps

802.11h - Espectro y Potencia en Europa - Banda 5 GHz

802.11i - Mejoras en Seguridad WIFI (WPA/WPA2)

802.11k - Mediciones y Gestión de RF en WIFI

802.11n - Transmisión de Datos - Altas Velocidades

802.11p - WAVE (WIFI en vehículos)

802.11r - Fast Roaming

802.11s - Redes Mesh / Wifi Municipal

802.11u - Internetworking con otras Redes

802.11v - Access Points, Gestión de Clientes (MIB)

802.11x- Seguridad, cifrado y encriptación

802.11w - Seguridad de Paquetes de administración.

1.4 Tecnologías en WLAN

Las WLAN, hacen uso de las ondas electromagnéticas para transmitir información de un punto a otro sin la existencia de conexiones físicas. Existen varias posibilidades empleadas en las WLAN para lograr esa transmisión. Una de ellas es por ondas infrarrojas (Infra Red), pero este método se limita a la línea de vista o a distancias cortas, y la otra es por ondas de radio frecuencia (RF), que son más usadas debido a que poseen más poder de penetración a través de los objetos que las IR. Las WLAN emplea la tecnología de *Espectro Extendido* (SS, *Spread Spectrum*) para modular las ondas de RF.

1.4.1 Espectro extendido (SS)

Esta técnica está estipulada por la FCC con el objetivo de minimizar la interferencia, tiene potencia de transmisión máxima de 1 watt y opera en al banda ISM. La tecnología de SS, consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una portadora concreta, lo que se hace es repartirla, por toda la banda disponible. Este ancho de banda total se comparte con el resto de usuarios que trabajan en la misma banda de frecuencia. El receptor del espectro extendido usa el conocimiento de cómo se hizo para comprimir la señal recibida y recuperar la señal de dato original. Proporciona gran robustez con respecto a la interferencia y al desvanecimiento resultante de la propagación de multitrayecto. Esta técnica tiene a su vez dos variantes: Salto de Frecuencia (FHSS) y Secuencia Directa (DSSS).

1.4.1.1 Espectro Extendido por Secuencia Directa (DSSS)

En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada, en una función de propagación determinada. El flujo de datos original, puede ser entonces recobrado en el extremo receptor, correlacionándolo con la función de propagación conocida. Esta técnica, consiste en la generación de un patrón de bits redundante llamado señal de chip para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante mediante una portadora de RF. En el receptor es necesario realizar el proceso inverso para obtener la señal de información original. (Bates, 2003)

1.4.1.2 Espectro extendido por salto de frecuencia (FHSS)

Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 MHz que son utilizadas por hornos de Microondas.

1.4.2 Otras tecnologías de radio de redes WLAN

Las WLAN no sólo utilizan las técnicas de espectro extendido, sino que también emplean: OFDM, CCK, CCK/OFDM y la *Codificación Convolutiva de Paquetes Binarios (PBCC, Packet Binary Code Convolutional)*; las dos primeras son de carácter obligatorio, mientras que las dos restantes son opcionales.

1.4.2.1 Multiplexación por División de Frecuencias Ortogonales (OFDM)

El sistema de multiplexación por división de frecuencias ortogonales, consiste, en enviar la información sobre un múltiplex de muchas portadoras “adecuadamente espaciadas” en frecuencia (Álvarez et al., 2005:181). La información puede ser modulada por la *Modulación de Amplitud en Cuadratura (QAM, Cuadratura Amplitud Modulation)* o en PSK. La ortogonalidad, posibilita que el espaciamiento entre portadoras sea óptimo, evitando la interferencia entre sí. Este espaciamiento consiste, en que la separación espectral entre portadoras consecutivas, sea siempre la misma e igual al inverso del período de símbolo. La utilización de las portadoras ortogonales permite por un lado lograr la identificación y el desvanecimiento selectivo y por otro obtener una mayor eficiencia espectral. La tecnología OFDM, permite además, eliminar la *Interferencia Inter Símbolos (ISI, Inter Symbol Interference)* y reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal, maneja muy bien el ruido y los cambios de impedancia. Como ventaja, simplifica el problema de propagación multitrayecto. La utilizan específicamente los estándares IEEE 802.11a e IEEE 802.11g y 802.11b.

En el caso del estándar IEEE 802.11a, las señales de datos son divididas en 52 subportadoras, separadas para proveer velocidades de transmisión de 6, 9, 12, 18, 24, 36, 48, ó 54Mbps. Para cada una de las subportadoras se utilizan técnicas de modulación como: BPSK, QPSK y QAM, en dependencia de la tasa de transmisión de los datos seleccionados como se puede apreciar en la tabla 1.1.

Tabla 1.1. Modulación y Codificación para razones de datos OFDM.

Razones de datos (Mbps)	Modulación	Razón de Código	Códigos de Bit por Subportadora	Códigos de Bit por símbolo OFDM	Datos de Bit por Símbolo OFDM
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16 QAM	1/2	4	192	96
36	16 QAM	3/4	4	192	144
48	64 QAM	1/2	6	288	192
54	64 QAM	3/4	6	288	216

Fuente: CommsDesign

En el caso de la norma IEEE 802.11g, la técnica OFDM cambia a la frecuencia a 2.4 GHz.

1.4.2.2 Conmutación de Códigos Complementarios (CCK)

Es un sistema de una sola portadora, donde todos los datos son transmitidos por la modulación de una sola frecuencia de radio o portadora. Constituye una variante a la modulación por conmutación de M alternativas ortogonales (*M-ary orthogonal keying*) y se basa en una constelación de portadoras fase y cuadratura, utilizando símbolos complejos. Es un método de codificación o la forma básica de modulación de la técnica DSSS usado en el estándar 802.11b para velocidades de 5.5 y 11 Mbps.

CCK, consiste en 64 símbolos de 8 chips de codificación modulados con DQPSK, comparado con la codificación de Barker que usa solo uno. Los bits de datos son codificados de forma diferente para las velocidades de 5.5 Mbps y 11 Mbps. Para la primera, 4 bits de datos son enlazados con una palabra de código, mientras que para la segunda son de 8 bits de datos. Cuando se utiliza CCK, el preámbulo/cabecera y la carga son transmitidos empleando CCK (Sotolongo y Poveda, 2006).

1.4.2.3 Conmutación de Códigos Complementarios/Multiplexación por División de Frecuencias Ortogonales (CCK/OFDM)

Constituye un método híbrido de codificación de espectro extendido. Está diseñado para facilitar el uso de las formas de onda de OFDM soportando compatibilidad con CCK. Además transmite el Preámbulo/Cabecera en una sola frecuencia de radio mediante CCK y la carga en múltiples frecuencias por medio de OFDM. Este híbrido representa una opción en el estándar IEEE 802.11g que está diseñado para evitar colisiones con las redes 802.11b que utilizan el método CCK.

Cuando se opera en la presencia de dispositivos Wi-Fi existentes, la cabecera CCK es transmitida para alertar a todos los dispositivos, que la transmisión está por empezar y para informar a estos dispositivos de la duración de la misma. La carga puede ser transmitida a una razón mucho mayor usando OFDM.

1.4.2.4 Codificación Convolutiva de Paquetes Binarios (PBCC)

Es una solución de simple portadora apoyada por Texas Instruments (TI). Emplea una señal de constelación más compleja 8-PSK comparada con la BPSK/ QPSK utilizada por CCK. Posee una estructura de codificación convolutiva en comparación con la estructura de codificación de bloque utilizada en CCK. Así, el mecanismo de decodificación, es completamente diferente. Al igual que CCK/OFDM, PBCC, se describe como un híbrido, utilizando CCK para transmitir la porción Preámbulo/Cabecera de cada paquete y PBCC para transmitir la carga. La máxima razón de datos que incluye PBCC para el estándar 802.11g, es de 33Mbps. Se debe señalar que PBCC fue incluido como un elemento optativo del estándar original IEEE 802.11b (Zyrem, 2001).

1.5 Bandas de Frecuencia

Las redes inalámbricas de área local hacen uso de las bandas ISM (*Industrial, Scientific and Medical*). Estas son bandas asignadas por Unión Internacional de las Telecomunicaciones (UIT), están reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industriales, científicas y médicas, y su uso está abierto a todo el mundo sin necesidad de licencia, respetando las regulaciones que limitan los niveles de potencia transmitida. Las bandas ISM están definidas en los rangos de 902–928 MHz

(banda 915 MHz), 2.4–2.4835 GHz (banda 2.4 GHz), y 5.725–5.85 GHz (banda 5.8 GHz) (Fig. 1.5). Las WLAN utilizan las dos últimas que se encuentran en el espectro de *Muy Alta Frecuencia* (VHF, *Very High Frequency*) y *Súper Alta Frecuencia* (SHF, *Super High Frequency*) respectivamente. (Sklar, 1998)

En EE.UU. también está definida una banda de uso libre en 5 GHz, la banda *Infraestructura de Información Nacional Sin Licencia* (UNII, *Unlicensed National Information Infrastructure*). En Europa, esta banda está sometida a restricciones para evitar interferencias con otros sistemas de radio. La banda UNII está formada por tres sub-bandas, UNII1 (5.15 - 5.25 GHz), UNII2 (5.25 - 5.35 GHz) y UNII3 (5.725 - 5.825 GHz) (Fig. 1.3).

El ancho de banda total disponible en la banda de 5 GHz es mayor que en la banda de 2,4 GHz (300 MHz por 83,5 MHz).

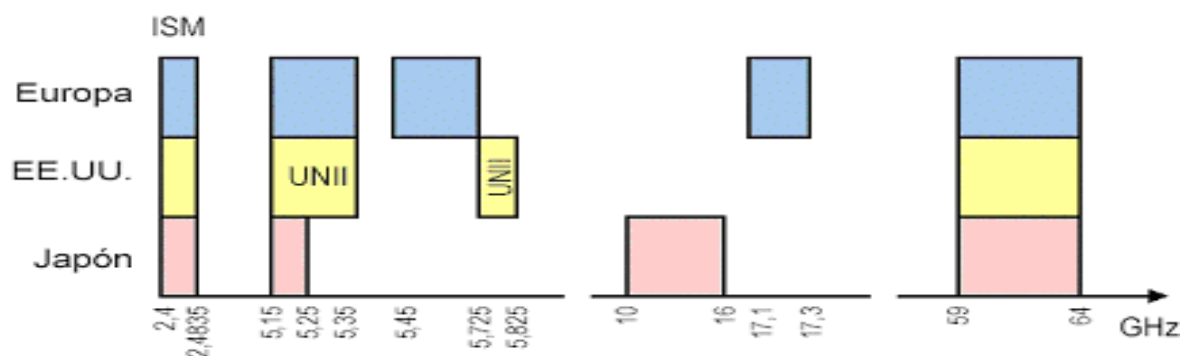


Figura 1.3. Bandas de frecuencias para WLAN.

1.6 Acceso al medio

El acceso es clave para la tecnología que se sustenta en el entorno de radio, por ser un medio compartido, al que todos los usuarios deben acceder. Los mecanismos de acceso se implementan sobre la capa MAC, de la capa de enlace. La capa MAC de IEEE 802.11 controla el acceso ordenado al medio mediante dos técnicas; la *Función de Coordinación Distribuida* (DCF, *Distributed Coordination Function*) y la *Función de Coordinación Puntual* (PCF, *Point Coordination Function*) (Redes de Acceso de Banda Ancha) Andueza Unanua, Angel M. 2003) (Bates, 2003)

1.6.1 Función de Coordinación Distribuida

La función de coordinación se define, como la funcionalidad que determina, cuándo una estación dentro de BSS está autorizada para transmitir y cuándo está habilitada para recibir unidades de datos de protocolo por el medio inalámbrico (León-García y Widjaja, 2005). Se encuentra en el nivel inferior del subnivel MAC y su funcionamiento se basa en técnicas de acceso aleatorias de contención por el medio. Utiliza como protocolo de acceso al medio *MACA (Multi Access Collision Avoidance)*, que no es más, que CSMA/CA con RTS (*Request to send*) y CTS (*Clear to send*), ésta es una variante del CSMA/CA.

- CSMA/CA: Cuando un nodo recibe un paquete a transmitir, primero escucha para asegurarse de que ningún otro está transmitiendo. Si el canal está despejado entonces transmite, si no, elige un factor aleatorio de retraso (*random back-off*) que determina el tiempo que debe esperar para poder transmitir. El nodo transmisor decrementará su contador de retraso durante los periodos en los que el canal esta libre. Cuando el contador de retraso alcanza el valor cero, el nodo transmite el paquete (Bates, 2003).

CSMA/CA en un entorno inalámbrico presenta dos problemas principales, el de los nodos ocultos cuando una estación cree que el canal está libre, pero está ocupado por otro nodo que no oye, y el de nodos expuestos cuando una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

MACA: Cuando se desea transmitir de una estación a otra primero se envía un paquete RTS a la otra, este paquete contiene el tamaño de la trama de datos que quiere transmitir. Si la otra estación acepta, responde con un paquete CTS que contiene una copia del tamaño de la trama de datos que le quiere transmitir la primera estación. Entonces, la primera estación esta libre para transmitir, y envía su trama e inicia su temporizador de espera del paquete de acuse de recibo, que le indicará que su trama fue recibida satisfactoriamente. Cuando la segunda estación recibe la trama de datos correctamente, le responde el acuse de recibo.

1.6.2 Función de Coordinación Puntual

Es una capacidad opcional que puede ser usada para proveer conexión orientada. Está asociada a las transmisiones libres de contención que utilizan técnicas de acceso deterministas. Está pensada para servicios de tipo sincrónico que no toleran retardos aleatorios en el acceso al medio. La función de PCF, es ejecutada por el *punto de coordinación*² en el punto de acceso dentro de un BSS, gestiona el acceso al medio mediante un proceso centralizado en el AP. Su funcionamiento se basa en ser compatible con el modo DCF. Los métodos de acceso PCF y DCF pueden operar conjuntamente dentro de una misma celda o conjunto básico de servicios.

1.7 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 (Hernando, 1995).

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.

1.7.1. 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.

² Se conoce como nodo organizador o director

- 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:

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

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. 1.4). 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 .

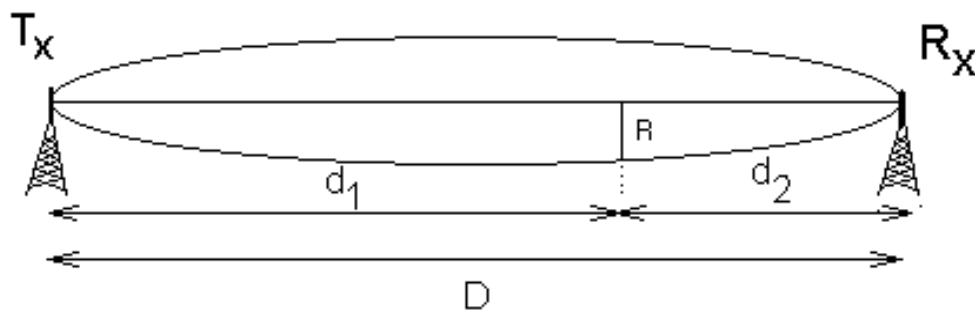


Figura 1.4. Primera zona de Fresnel.

En la práctica es necesario que al menos el 60% de la primera zona de Fresnel esté libre de obstáculos. La tabla 1.2 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.

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

Tabla 1.2 Atenuación en función de la clarencia.

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 pérdidas 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.

1.8 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).

1.8.1 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.

1.8.2 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 (Fig. 2.2). 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 Hernando (1995), 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. (Wang y Poor, 2003)

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 (Matos, 2005).

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. (Ramos, 2005)

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 (García Fernández, 2005).

- **Distorsión por Multitrayecto:** 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.

1.9 Análisis de las características de un radioenlace.

Un enlace de radio consta de tres componentes fundamentales: el transmisor, el receptor y el canal aéreo. El transmisor es el responsable de modular una señal digital a la frecuencia

utilizada para transmitir, el canal aéreo representa un camino abierto entre el transmisor y el receptor, y el receptor es el encargado de capturar la señal transmitida y llevarla de nuevo a señal digital. El factor limitante de la propagación de la señal en enlaces de microondas es la distancia que se debe cubrir entre el transmisor y el receptor, además, esta distancia debe ser libre de obstáculos en algunos casos. Otro aspecto que se debe señalar es que en estos enlaces, el camino entre el receptor y el transmisor debe tener una altura mínima sobre los obstáculos en el trayecto.

Un radioenlace está caracterizado por tres elementos básicos:

- Energía efectiva emitida o potencia radiada: En ella intervienen la energía emitida o potencia del transmisor, las pérdidas (cables y conectores) y la ganancia de la antena transmisora.
- Pérdidas en la propagación: Dependen de las condiciones de propagación.
- Sensibilidad efectiva de recepción: Depende de la ganancia de la antena receptora, de las pérdidas en los cables y la sensibilidad del receptor.

1.10 Tipos de antenas

Existen diferentes tipos de antenas, cada una de las cuales tiene una aplicación y entorno de uso específico, ofreciendo una capacidad de cobertura determinada. Normalmente, bajo las mismas condiciones del enlace, a medida que la ganancia de una antena se incrementa se alcanzan distancias de cobertura mucho mayores, pero sólo en una dirección determinada. En el Anexo (II, III, IV, V) aparecen figuras de los distintos tipos de antenas (omnidireccionales, sectoriales o directivas).

1.10.1 Antenas Direccionales

Son capaces de enfocar toda la señal que le aplica la tarjeta o punto de acceso, a una dirección concreta, con mayor o menor grado de directividad en función del modelo y características (Fig. 1.5). Normalmente se usan para establecer enlaces punto a punto o para enlazar con un nodo que tenga una antena Omnidireccional. El ancho del haz, es angosto. Tienen la ganancia alta por lo tanto se utilizan para enlaces a larga distancia. Existen varios

tipos de antenas direccionales o directivas como son las Yagi, las biquad, las de bocina, las helicoidales, las antenas path, los platos parabólicos, etc.

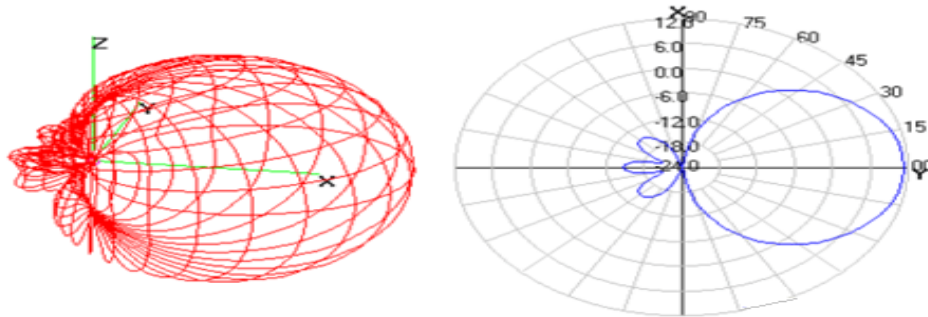


Figura 1.5. Patrón de radiación de una Antena Direccional.

1.10.2 Antenas Omnidireccionales

Están diseñadas para proveer un patrón de radiación de 360° (Fig.1.6). Propagan la señal de RF en todas las direcciones en el plano horizontal, aunque tienen un rango limitado en el plano vertical.

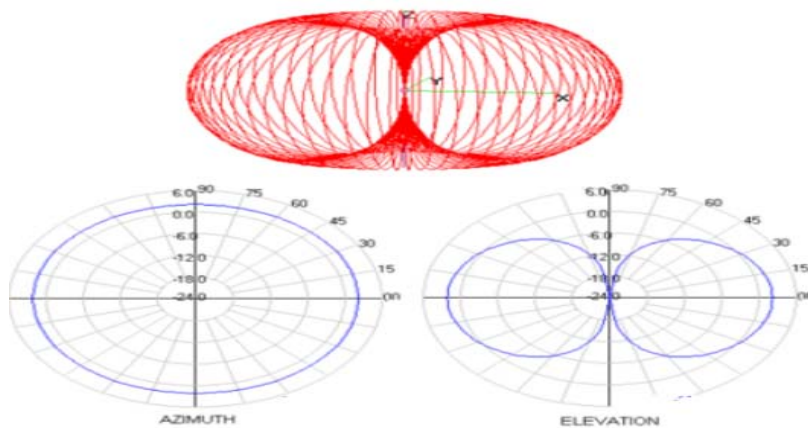


Figura 1.6. Patrón de radiación de una Antena Omnidireccional.

Son las más comunes en WLAN y se utilizan cuando se requiere dotar de cobertura en todas las direcciones. Proporcionan la cobertura más amplia dentro de edificios, pudiendo formar celdas circulares muy poco solapadas a lo largo del edificio. La mayoría de los puntos de acceso estándar disponen de una antena omnidireccional de baja ganancia. Los

tipos más usados actualmente de antenas omnidireccionales son los dipolos y las de plano de tierra.

1.10.3 Antenas Sectoriales

Irradian principalmente en un área específica. El haz puede ser tan amplio como 180 grados, o tan angosto como 60 grados. Las antenas sectoriales se utilizan cuando se necesita conectar lugares distantes y de área extensa. Cubren un ángulo mayor, se que se conoce como sector. Tiene mayor alcance que las antenas omnidireccionales y menor que las direccionales (Ver Anexo V).

1.11 Sensibilidad del receptor

Constituye un aspecto importante en el receptor, ya que éste tiene un umbral (*threshold*) mínimo de energía recibida (en el conector de la tarjeta) para el cual la señal tiene que alcanzar una cierta tasa de transmisión (*bit rate*). Si la energía de la señal es menor que la máxima tasa de transmisión, entonces, se decrementará el rendimiento, por lo que es mejor el empleo de equipos con un valor de umbral bajo.

1.11.1 Relación señal a ruido

La relación señal a ruido (C/N) es la mínima diferencia de potencia que se debe alcanzar entre la señal recibida y el ruido (ruido térmico, ruido industrial debido a los microondas y ruido debido a otra WLAN en la misma banda de frecuencias). Es la que define la calidad de la señal recibida. Se define como el cociente entre la potencia de señal y la potencia de ruido ambas en Watt. La expresión matemática es la siguiente:

$$C/N = \frac{P_r}{KTB} \quad (1.2)$$

Donde K es la constante de Boltzman, T la temperatura y B el ancho de Banda

1.11.2 Margen

El término de margen (*M*) se introduce para compensar el desvanecimiento y se define por el cociente entre la relación portadora a ruido de operación *C/N* y $(C/N)_0$, este último es el valor requerido del diseño para cumplir con una determinada calidad de servicio (*QoS*).

Quedando la expresión de la siguiente forma:

$$M = \frac{C/N}{(C/N)_0} \geq 1 \quad (1.3)$$

Un buen radioenlace debe tener de 5 a 17 dB de margen.

1.12 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. (Earte, 2006). A continuación se profundiza en aspectos contenidos dentro de la seguridad en este tipo de redes.

1.12.1 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 autenticación 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 autenticación mediante el envío de una trama de autenticación. Una vez realizada ésta, la estación cliente envía una trama asociada y el AP responde con otra. (Cors y Pernich, 2006)

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 *confidencialidad*, *integridad*, *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 “hotspot” públicos para recopilar información sensible del sistema.

-Escuchas e interceptación: 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.

1.12.2 Mecanismos de seguridad

1. 12.2.1 Autenticación y control de acceso

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 (*beacon frame*)³ 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 *beacon frame* (Alonso, 2006). 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 interconectadas para autenticar los dispositivos conectados a un puerto LAN. Permite el transporte de tramas de *Protocolo de Autenticación Extensible (EAP*⁴, *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

³ Tramas cortas transmitidas para proporcionar: reloj (sincronización de tiempos), parámetros de FH o DS, SSID, mapa de indicación de tráfico y tasas de transmisión soportadas

⁴ 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*)

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 mas 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 (Figueroa y Merino, 2004). 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 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. (Caballé, 2005)

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 autenticación, 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 autenticación 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 Encryption 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 Protocol*) en lugar de los códigos MIC. WPA2 incluye soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

1.13 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 IEEE, 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, 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 pérdidas 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.

Capítulo II. DISEÑO DEL ENLACE

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 y que la calidad de servicio sea superior 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 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 Situación de la red UCLV

El diseño y proyección de la red UCLV data de 1998 y su instalación según la concepción inicial concluyó en mayo del 2000. Todos los tramos que unen el nodo central y los edificios son de fibra óptica multimodo de tipo 62.5/125. En el año 2002 se realiza la segunda expansión de la Red UCLV a las áreas más lejanas del centro de la fibra óptica igualmente usando fibra multimodo de 62.5/125. En esta expansión se beneficiaron las Facultades de Ciencias Agropecuarias y de Construcciones logrando el acceso a la Intranet universitaria. Además se conectaron otras zonas como el SEDER y el Centro de Bioactivos Químicos (CBQ), el Instituto de Biotecnología de las Plantas (Fig. 2.1) y más recientemente se han unido áreas como la Dirección de Transporte, la casa de la FEU, la dirección de Becas y la casa VLIR que patrocina el proyecto que tiene la UCLV con las Universidades Flamencas Belgas y está ubicado en el área de las Antillas. Esta última unión se realizó con fibra monomodo de 9 micras

La Universidad Central de la Villas cuenta hoy con una gran red de computadoras, con 14 enlaces principales y un total de 7 Km. de fibra óptica. Se brindan los servicios principales de correo electrónico nacional e internacional y acceso a Internet para todos los profesores y estudiantes y tiene una Intranet bien consolidada donde están representadas todas las áreas universitarias. Los usuarios, además acceden a otras aplicaciones y servicios que son vitales para el trabajo docente e investigativo que en la misma se realizan.

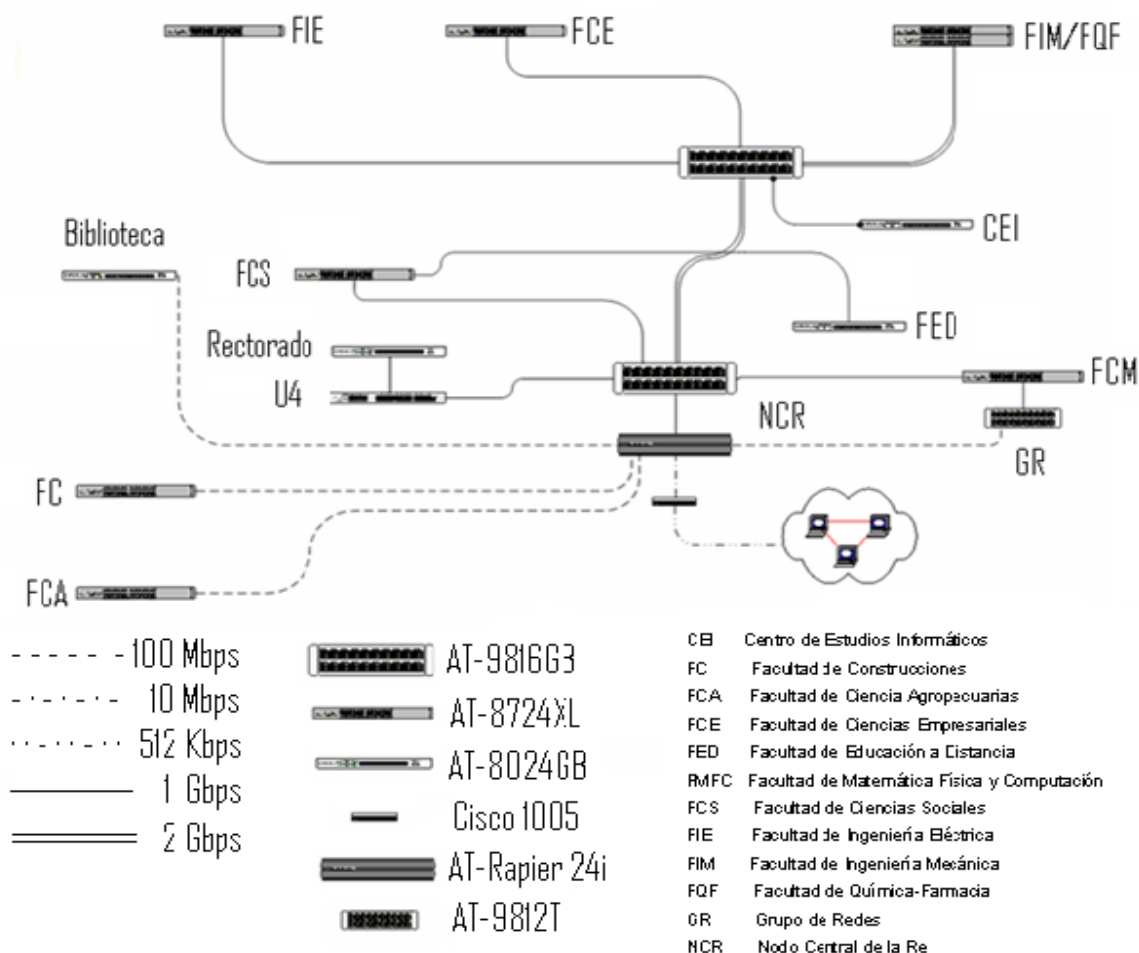


Figura 2.1. Distribución actual del Backbone de la UCLV.

Desde que la Red UCLV fue diseñada quedaron algunos lugares importantes que no se incluyeron principalmente por limitaciones económicas. Con el paso del tiempo ha aumentado la necesidad de que estos lugares queden definitivamente unidos a la red UCLV y aprovechando el desarrollo de las nuevas tecnologías inalámbricas se decide unir el

centro de Investigación ubicado en el Jardín Botánico con la Facultad de Ingeniería Eléctrica.

Centro de Investigación del Jardín Botánico

El Jardín Botánico es el único de su tipo en la provincia de Villa Clara, dentro del mismo se encuentra un Centro de Investigación de gran importancia adjunto a la UCLV. La remodelación de este lugar está amparada por el proyecto VLIR en conjunto con el gobierno de Villa Clara. Con este Centro de Investigación se pretende alcanzar el desarrollo de la naturaleza de diferentes especies oriundas de varias latitudes del planeta y un lugar de esparcimiento natural.

El Centro de Investigación presenta una pequeña red interna, contando en la actualidad con siete computadoras. Como no se encuentra unida a la red universitaria, no tiene acceso a ninguno de los servicios ofrece la intranet universitaria, ni a los servicios nacionales, ni internacionales de correo e internet. El servicio de correo electrónico se realiza mediante una conexión vía módem, que en estos momentos presenta problemas.

2.1.1 Análisis del entorno para enlazar la red con infraestructura cableada

Para conectar este centro a la red de la Universidad la primera alternativa es implementar una infraestructura cableada. El lugar más cercano con el cual se puede enlazar esta subred es la Facultad de Ingeniería Eléctrica (FIE), se debe realizar un enlace entre ellos mediante fibra óptica. Para la realización del mismo es necesario analizar las condiciones del terreno entre ambos lugares.

El Centro de Investigación es una edificación pequeña de apenas un piso de entre dos y tres metros de altura, se encuentra en una zona baja y rodeado de árboles que lo rebasan. Por su parte la Facultad de Ingeniería Eléctrica es un edificio alto, de cuatro pisos, cada uno de ellos de aproximadamente un poco más de tres metros, que se encuentra en una zona alta de la Universidad, en uno de sus lados la vegetación que existe no rebasa su altura. En línea recta con el Jardín Botánico se observa que el terreno es bastante irregular, aunque no existen grandes elevaciones, presenta altas y bajas, además de varios puntos de mediana vegetación, el terreno en ocasiones se ha utilizado como zona de cultivos. La distancia que existe entre los dos puntos es de 518m según el cálculo que se hizo con el programa Google Earth y que aparece en el Anexo VII. Por otro lado, la carretera que sirve de tránsito para

el desplazamiento desde la FIE hacia el Jardín Botánico no es uniforme y en sus alrededores presenta zanjas con agua corriente de mediana profundidad. Agregando que los dos centros no se encuentran del mismo lado de esta carretera. Otro aspecto importante es que el lugar donde radica el Centro de Investigación está rodeado de abundante vegetación, con árboles de gran tamaño. Por las características que presenta el trayecto la implementación de una red LAN de infraestructura cableada no es una solución viable, por lo que surge la necesidad de buscar otras alternativas.

2.1.2 Enlace inalámbrico

Por el avance que presentan las redes inalámbricas de área local y las ventajas que ofrecen frente a una red con cables, y las limitaciones que tienen estas, se decide adoptar las WLAN para dar solución al problema de la conexión de estos lugares y de esta contribuir al completamiento de la red universitaria y que este Centro de Investigación tenga acceso a todos los servicios que brinda. Este reto se asume teniendo en cuenta el apoyo que tiene la UCLV con el Proyecto VLIR (*Vlaamse Interuniversitaire Raad*) de las Universidades Flamencas de Bélgica que se encargan del financiamiento.

2.2 Diseño del enlace inalámbrico

Para realizar un diseño correcto de una red WLAN, es necesario analizar una gran variedad de parámetros y pasos a tener en cuenta.

Para conectar las redes LAN de la FIE y el Centro de Investigación del Jardín Botánico de manera inalámbrica, se realiza un enlace punto a punto. Estos enlaces se utilizan para conectar dos puntos que se encuentran en lugares diferentes. Se necesita una visión libre de obstáculos de la trayectoria entre los puntos. Se coloca un punto de acceso en el Centro de Investigación y el otro en la FIE.

El primer paso para el diseño es demostrar si se cumplen las condiciones de tierra plana.

2.2.1 Demostración de tierra plana

$$d_0[km] = \frac{80}{\sqrt[3]{f(MHz)}} \quad (2.1)$$

Si la distancia que existe entre los puntos a enlazar es menor que d_0 , entonces, se cumple la condición de tierra plana. Se pueden hacer los cálculos para los diferentes canales en que se divide la banda de frecuencia en que opera el equipo. Para este se escogió la frecuencia correspondiente al último canal de Estados Unidos (canal 11 $f = 2462\text{MHz}$) (Ver Anexo VIII), sustituyendo en la expresión el resultado es el siguiente:

$$d_0[km] = \frac{80}{\sqrt[3]{2462}} = 5.9426km$$

Como la distancia entre la FIE y el Centro de Investigación es menor que el resultado anterior, entonces se cumple la condición. Estos equipos pueden usar cualquier canal de la banda de frecuencia solo depende del tipo de norma que establece el país donde se instala el enlace.

2.2.2 Distancia entre los puntos.

Para saber si la distancia entre los dispositivos es menor que la distancia de alcance máxima del equipo, se tienen en cuenta una serie de parámetros que intervienen en la expresión que se muestra a continuación:

$$L_{bf}(dB) = 32,45 + 20\log f(MHz) + 20\log d(km) \quad (2.2)$$

Despejando llegamos a

$$20\log(D) = P_{T_x} - P_{req} + G_{R_x} + G_{T_x} - 32.45 - 20\log(f) \quad (2.3)$$

Esta ecuación no incluye el valor del margen.

La f se refiere a la frecuencia, una vez seleccionada la banda de frecuencia donde trabaja el equipo inalámbrico, es necesario, seleccionar un canal con su respectivo valor de frecuencia, estos valores dependen del país donde se implante la red inalámbrica (Ver Anexo VIII), en esta expresión la frecuencia está en MHz. Los términos G se refieren a las ganancias de las antenas transmisora y receptora, y los términos de P se refieren a las potencias de la antena transmisora y la potencia requerida en el receptor. Como la antena viene integrada en el equipo las pérdidas en los cables son despreciable, entonces la

potencia que sale del equipo es la de la antena. Otros elementos importantes en la determinación de la distancia son:

- la relación señal a ruido
- la sensibilidad del receptor
- la figura de mérito
- el margen
- la atenuación en los cables

Esta expresión da como resultado la distancia máxima a la que pueden estar las antenas en dependencia de los términos. La distancia que se obtiene está en kilómetros.

Los cálculos se realizan para casos límites de frecuencia, potencia del transmisor y sensibilidad del receptor, usando la expresión (2.3) y utilizando:
 $X(dBW) = Y(dBm) - 30dBW$ para convertir de dBm a dBW.

Para la frecuencia del canal 11 $20 \log(f(MHz)) = 20 \log(2462) = 67.83dBHz$

➤ Potencia del transmisor de 38 dBm (8 dBW)

Sensibilidad del receptor de -65 dBm (-95 dBW) y una razón de transmisión de 54 Mbps.

$$20 \log(D) = 8dBW - (-95dBW) + 18dbi + 18dB_i - 32.45 - 67.83dBHz$$

$$20 \log(D) = 38.72dB - Margen(17dB)$$

$$D = 12.19 Km.$$

Sensibilidad del receptor de -82 dBm (-112 dBW) y una razón de transmisión de 6 Mbps.

$$20 \log(D) = 8dBW - (-112dBW) + 18dB_i + 18dB_i - 32.45 - 67.83dBHz$$

$$20 \log(D) = 55.72dB - 17dB$$

$$D = 86.9 Km.$$

➤ Potencia del transmisor de 45 dBm (15 dBW)

Sensibilidad del receptor de -65 dBm (-95 dBW) y una razón de transmisión de 54 Mbps.

$$20 \log(D) = 15dBW - (-95dBW) + 18dB_i + 18dB_i - 32.45 - 67.83dBHz$$

$$20\log(D) = 45.72dB - 17dB$$

$$D = 27.3 \text{ Km.}$$

Para la frecuencia del canal 1 $20\log(f(\text{MHz})) = 20\log(2412) = 67.65\text{dBHz}$

➤ Potencia del transmisor de 38 dBm (8 dBW)

Sensibilidad del receptor de -65 dBm (-95 dBW) y una razón de transmisión de 54 Mbps.

$$20\log(D) = 8\text{dBW} - (-95\text{dBW}) + 18\text{dbi} + 18\text{dBi} - 32.45 - 67.65\text{dBHz}$$

$$20\log(D) = 38.9\text{dB} - 17\text{dB}$$

$$D = 12.44 \text{ Km.}$$

Sensibilidad del receptor de -82 dBm (-112 dBW) y una razón de transmisión de 6 Mbps.

$$20\log(D) = 8\text{dBW} - (-112\text{dBW}) + 18\text{dBi} + 18\text{dBi} - 32.45 - 67.65\text{dBHz}$$

$$20\log(D) = 55.72\text{dB} - 17\text{dB}$$

$$D = 86.3 \text{ Km.}$$

➤ Potencia del transmisor de 45 dBm (15 dBW)

Sensibilidad del receptor de -65 dBm (-95dBW) y una razón de transmisión de 54 Mbps.

$$20\log(D) = 15\text{dBW} - (-95\text{dBW}) + 18\text{dBi} + 18\text{dBi} - 32.45 - 67.65\text{dBHz}$$

$$20\log(D) = 45.9\text{dB} - 17\text{dB}$$

$$D = 27.86 \text{ Km.}$$

Los cálculos pueden ser comprobados mediante una hoja de cálculo (Ver Anexo IX).

Tabla 2.1 Resultados del cálculo de las distancias

Frecuencia	Potencia del Tx	Sensibilidad	Distancia
2412 MHz	38 dBm (8 dBW)	-65 dBm (-95 dBW)	12.19 km.
		-82 dBm (-112 dBW)	86.9 km.
	45 dBm (15 dBW)	-65 dBm (-95 dBW)	27.3 km.
2462 MHz	38 dBm (8 dBW)	-65 dBm (-95 dBW)	12.44 km.
		-82 dBm (-112 dBW)	86.3 km.
	45 dBm (15 dBW)	-65 dBm (-95 dBW)	27.86 km.

Como conclusión la distancia entre los puntos a enlazar está dentro del rango de la distancia de alcance máximo, no existen problemas para que la señal llegue al receptor por falta de cobertura.

2.2.3 Altura de los Equipos

Para determinar la altura a la que deben ser colocados los radios en los puntos a enlazar, hay que garantizar que haya línea de vista libre, y que la altura del obstáculo más crítico entre ambos no interfiera dentro el 60% de la primera zona de Fresnel. Se instalará una torre atirantada en el Centro de Investigación por estar ubicado en una zona más baja que la FIE, además porque cuenta con un solo piso. En el tope de esta torre se colocará uno de los equipos de radio para exterior, mientras que en el edificio de la FIE por tener 18m altura (con cuatro pisos) no se utilizará torre atirantada, el otro equipo se soportará en el techo del extremo izquierdo del edificio tendiendo en cuenta que ambos equipos estén en la misma línea de vista.

2.2.4 Determinación de la primera zona de Fresnel

El resultado de la primera zona de Fresnel se obtiene aplicando la expresión (1.1), en esta expresión interviene la distancia del obstáculo crítico al transmisor y al receptor. El área donde mayor número de obstáculos críticos existen, que pueden afectar la primera zona de Fresnel es la que rodea el Centro de Investigación, entre los que sobresalen dos Pinos y un árbol de gran tamaño, aunque ninguno sobrepasa los 17 metros de altura y se encuentran a una distancia de 15 metros del equipo de la casa, también existe un grupo de árboles del lado derecho de la vía que conduce al Jardín Botánico, pero estos son de menor tamaño y vistos desde el piso superior del edificio de la FIE no son capaces de obstruir.

Para la frecuencia de 2 462 MHz (Canal 11), $\lambda = \frac{300}{2462} = 0.122$ metros.

$$R = \sqrt{\frac{0.122 * 15 * 503}{518}} = 1.33 \text{ metros}$$

De éste radio el 60% de despeje es 0.798 metros.

Para la frecuencia de 2 412 MHz (Canal 1), $\lambda = \frac{300}{2412} = 0.124$ metros

$$R = \sqrt{\frac{0.124 * 15 * 503}{518}} = 1.34 \text{ metros}$$

De éste radio el 60% de despeje es 0.804 metros.

La primera zona de Fresnel debe estar por encima del obstáculo crítico, que en este caso mide alrededor de 17 metros. Como conclusión se propone ubicar una torre a 19 metros del suelo en el Centro de Investigación, en la cual estará el radio de exterior y en la FIE se ubicará el otro sin la utilización de una torre en la azotea a una altura de 18 metros.

Con ayuda del MatLab y realizando un estudio del terreno se pudo obtener una estimación del radio de la primera zona de Fresnel (Fig. 2.2).

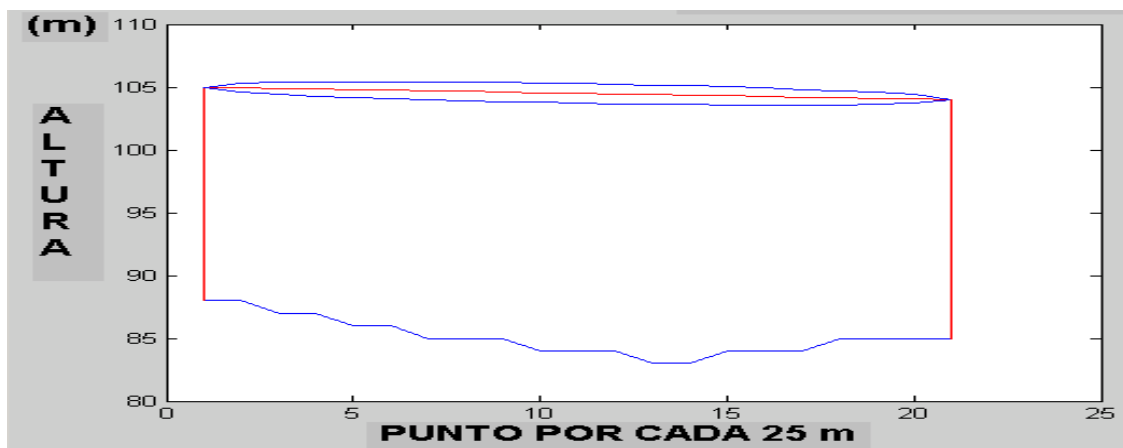


Figura 2.2 Análisis del radio de la zona de Fresnel utilizando MatLab.

En el Anexo X se puede observar también la zona de Fresnel calculada por un software Profesional llamado Cobra, utilizado por Copextel Nacional para el diseño de redes inalámbricas.

2.3 Oferta del equipamiento

Una vez planteada la solución es necesario seleccionar el equipamiento adecuado, valorando para esto aspectos de costo, interoperabilidad con otras tecnologías que se encuentren funcionando en el lugar aplicable al entorno. Para la adecuada selección se realiza un análisis detallado de las ofertas del mercado mundial y nacional.

Mercado Mundial

En el mercado mundial innumerables son las ofertas que se brindan de puntos de acceso y puntos de acceso con la función de puentes, para exteriores e interiores, tarjetas inalámbricas y antenas que pueden estar integradas o no al punto de acceso (Ver Anexos I, II, III, IV, V). Son varias las empresas, firmas, consorcios, etc. que se dedican a la producción y comercialización de los implementos para redes inalámbricas. Entre estas empresas están: Alvarion, Tsunami, SparkLan, SmartBridge, Lucent, Linksys, Nokia, 3Com, FreeCon, Cisco, KBest entre otros. (Tsunami Quickbridge Wireless Radio Outdoor, 2002).

Tabla 2.2. Características de algunos productos inalámbricos para exterior.

Wave Access	Quick Bridge	Breeze Access														
<ul style="list-style-type: none">• Razón de Datos 3.2 Mbps y 1.6 Mbps• Máxima Potencia de Salida 17 dBm• Sensibilidad en el receptor 86dbm QPSK 16QAM 74dbm• Rangos de Operación Antena<table><tr><td>3.2Mbps</td><td>6Mbps</td></tr><tr><td>20</td><td>10Km 30Km</td></tr><tr><td>16</td><td>6Km 24Km</td></tr><tr><td>10</td><td>3Km 12Km</td></tr></table>• Tecnología FHSS con modulación 16QAM y QPSK• Banda de Frecuencia de 2.4 GHz	3.2Mbps	6Mbps	20	10Km 30Km	16	6Km 24Km	10	3Km 12Km	<ul style="list-style-type: none">• Razón de datos 18 Mbps y 12 Mbps• Potencia de Salida 16 dBm máximo 15 dBm típico• Antena Integrada 20dBi• Máxima Sensibilidad en el receptor: -20 dBm libre de error.• Modo de Operación: Multiplexación por División en el Tiempo• Técnica de Modulación QPSK• Banda de Frecuencia de 5 GHz• Distancia Máxima 10 Km con línea de vista.	<ul style="list-style-type: none">• Razón de Datos 3 Mbps• Potencia de salida 26 dBm 2 dBm.• Antena 15dB• Sensibilidad<table><tr><td>1 Mbps</td><td>-87 dBm</td></tr><tr><td>2 Mbps</td><td>-81 dBm</td></tr><tr><td>3 Mbps</td><td>-73 dBm</td></tr></table>• Modo de Operación: Multiplexación por División en el Tiempo• Técnica de Acceso FHSS CSMA/CA• Modulación Multi nivel GFSK• Banda de Frecuencia 2.4GHz	1 Mbps	-87 dBm	2 Mbps	-81 dBm	3 Mbps	-73 dBm
3.2Mbps	6Mbps															
20	10Km 30Km															
16	6Km 24Km															
10	3Km 12Km															
1 Mbps	-87 dBm															
2 Mbps	-81 dBm															
3 Mbps	-73 dBm															

Fuente: Lucent Technologies, Proxim y Alvarion (Wave ACCESS NET, 1999; Breeze Access TM II., 2004; MicroAlcarria, 2007)

Oferta en Cuba

En Cuba la corporación Copextel comercializa equipamiento electrónico de alta tecnología. La empresa tiene como filosofía de trabajo la integración de todas sus tecnologías en forma de un único paquete que comercializa “llave en mano”. Esta modalidad cubre todas las etapas, desde el proyecto inicial, instalación y puesta en marcha, hasta los servicios de post venta y es quien asumirá el montaje y puesta en marcha de este enlace.

No obstante en Cuba, al igual que en todos los países, existe una reglamentación para la concepción, diseño e instalación de redes inalámbricas, establecida por la Agencia de Control y Supervisión del Ministerio de Informática y Comunicaciones, MIC.

En particular los requerimientos técnicos para la selección del correspondiente equipamiento también están normados. A continuación se relacionan los principales:

Los equipos a emplear estarán limitados a una potencia de salida máxima de 100 mW y la potencia isotropa radiada equivalente (p.i.r.e) de cualquier instalación no podrá superar los 200 mW.

Los equipos que operen en las frecuencias entre 2456 y 2483,5 MHz podrán emplear valores de p.i.r.e superiores, cuando ello se justifique en beneficio de objetivos de interés nacional, atendiendo a la siguiente distribución:

$$Pr = 20 + 10\text{Log}(360/D) \text{ dBm}; \quad \text{donde:}$$

D = la anchura del lóbulo principal de la antena entre puntos a -3 dB

Pr = p.i.r.e = producto expresado en dB de la potencia suministrada a la antena transmisora multiplicada por la ganancia directiva de la misma relativa a un radiador isotrópico

Pr está limitada a un valor máximo de 36 dBm para estos casos.

Los equipos que se pretenda se guiarán en los restantes aspectos técnicos por las disposiciones del estándar IEEE 802.11 y sus correspondientes ampliaciones y modificaciones IEEE 802.11b, IEEE 802.11b/cor-1 e IEEE 802.11g, en correspondencia con la modalidad de acceso al espectro y las velocidades máximas de transmisión.

2.4 Selección del equipamiento

Después de hacer un estudio de mercado de las diferentes ofertas, en conjunto con la empresa comercializadora Copextel, se decidió usar equipos K-BEST, en específico, la serie BL 3201 procedente de Corea, pues son los que presentan un comportamiento más estable y seguro de los que se importan en estos momentos. Además son los proveedores que mejor garantía proporcionan en cuanto a la entrada de este tipo de equipamiento al país, pues por la situación existente en Cuba con el bloqueo americano está limitada la entrada al

país de la mayoría de las firmas que comercializan este tipo de tecnología. Este equipo tiene un alcance de hasta de 60 Km según los catálogos del fabricante conectándose en líneas de vista libres, con una antena integrada, pero las velocidades de conexión son bajas del orden de los 2 Mbps aunque en la práctica las máximas velocidades se alcanzan hasta los 4 Km aunque pueden variar dependiendo entre otros de factores climáticos. Como la distancia entre el Jardín Botánico y la FIE es menor que la distancia máxima permisible por el equipo, surge la interrogante de si el enlace está sobre diseñado. Desde el punto de vista práctico no existen otras alternativas en cuanto a la selección, por la poca accesibilidad que tienen las empresas cubanas al mercado mundial, pero tiene la ventaja que este equipo puede ser aprovechado en posteriores proyectos inalámbricos en la Universidad. El equipamiento está comprado con todos los accesorios necesarios para ejecutar el enlace.

2.5 Características del K-BEST

K-BEST diseña, desarrolla, fabrica y manufactura toda clase de transmisores, receptores y transceptores de Microondas, Radio y Satélite en las telecomunicaciones inalámbricas. Entre los productos K-BEST se encuentran puentes inalámbricos de microondas (*Microwave Wireless Bridge*), transmisores, receptores, entre otros (Ver Anexo XI). Estos dispositivos cubren el rango de frecuencia de 10 MHz a 50GHz. La tecnología K-Best se utiliza en telecomunicaciones inalámbricas, transmisiones satelitales, como estaciones base-móviles, como conexiones de radio punto a punto, como sistemas punto a multipunto, en técnicas de transmisión de audio y video, y en cobertura militar. La mayoría de los productos comunes son soluciones WLAN para exterior (IEEE 802.11a / IEEE 802.11b / IEEE 802.11g) y amplificadores WLAN para exterior (2.4 GHz, 5.8 GHz), entre otros. (K-BEST Tech Wlan Solutions, 2005). Con capacidades de transmisión de: 2xE1, 4xE1, 8xE1, 16xE1, E3, (21 x E1) DS3 y STM-1. Para la tasa fija (Punto a Punto) y IEEE 802.11a, /802.11b y /802.11g para la tasa fija/variable (Punto a Multipunto) con QoS.

Series BL 3 000-3010, BL3200

Cada serie es un equipo con características técnicas diferentes para sistemas wireless en exteriores que ofrecen una excelente comunicación de banda ancha. Este sistema se usa para soluciones de RF punto a punto y punto a multipunto, que conectan múltiples LAN

entre diferentes edificios. Soportan razones de datos por encima de 11Mbps utilizando la tecnología de espectro extendido por secuencia directa (DSSS). Los equipos de esta serie están diseñados para altas razones de datos y puentes para exteriores de largas distancias, que trabajan en la banda de 2.4 a 2.5 GHz utilizando las tecnologías de radio OFDM y DSSS. En el Anexo XII se muestran variedades de equipos de la firma KBest que se comercializan en Cuba.

Datos del K-BEST BL-3201 802.11 b/g Outdoor radio

Este es un equipo para enlaces punto a multipunto. Es compatible con el estándar IEEE 802.11b trabaja de forma mixta (802.11b/g). Tecnología bi-direccional. La velocidad se ajusta automáticamente y tiene una señal de LED que indica ayuda para alinear la antena

Canales de operación: FCC (1~11 canales), para Estados Unidos, ETSI (1~13 canales), para Europa y Japón (14 canales).

Potencia de salida: 38dBm / 45dBm

Potencia del equipo: 0.1 w a 0.5 para las frecuencias de 2400 y 2483 MHz.

Sensibilidad del receptor:

Tabla 2.3. Valores de Sensibilidad del receptor para el K-BEST BL 3201.

Sensibilidad (dBm)	Tasa de Transmisión (Mbps)
-65	54
-66	48
-70	36
-74	24
-77	18
-79	12
-81	9
-82	6

Administración: Herramientas de manejo basado en Windows, en Web y en Telnet.

Modo de Operación: Puede ser configurado en tres modos de trabajo: Estación, Punto de Acceso (AP) y Punto de Acceso con repetidor (WDS).

Protocolos: TCP/IP, IPX/SPX, NetBEUI

Seguridad: Tiene un manejo poderoso de seguridad, basado en: encriptación WEP 64/128 bits, WEP ASCII/Hexadecimal, WPA WPA-PSK y filtrado de direcciones MAC

Ambiente: Temperatura de Operación: -10°C~60°C

Temperatura de almacenamiento: -30°C~80°C

Humedad: 5%~95% sin condensación

Fuente de alimentación: AC 100-264V, DC 15V, 50-60Hz

Datos Físicos: Las Dimensiones son 50 (w) × 350 (d) × 95 (h); mm y un peso de 4.3 Kg.

Especificaciones para las antenas integradas de panel:

- Ganancia: 18dBi
- Ancho del Haz: H17 E11
- VSWR (Razón de onda estacionaria) ≤ 1.4
- Razón *Front to Back* (FTBR) > 30
- Impedancia: 50Ω
- Garantía: Limitado por un año.

Existen especificaciones que da el fabricante de las velocidades de conexión que se logran con el equipo según el tipo de modulación de la señal que se use. Ver Anexo XIII. En el Anexo XIV aparece un gráfico que muestra como en la medida que las distancias entre los equipos es mayor va disminuyendo la velocidad máxima de conexión que alcanza el enlace y es necesario ir cambiando el tipo de modulación de la señal para lograr que los equipos se conecten.

2.6 Análisis económico

Para el análisis económico se analiza el precio de cada uno de los materiales y el costo de mano de obra para la posterior puesta en marcha. En las tablas 2.4 y 2.5 se muestran los precios de los materiales y de la instalación y puesta en marcha respectivamente. Estos equipos aún caros por la novedad tecnológica, con el tiempo disminuyen el costo.

Tabla 2.4. Componentes y precios para el enlace.

Descripción	Precio CUC	Precio MN	Cant.	Total CUC	Total MN
KBEST BL3201	\$1416.45	\$424.94	2	\$2832.90	\$849.87
Protector Polyphaser IW-2H2DC48/W	\$125.00	\$37.50	2	\$250.00	\$75.00
Cable de tierra Verde/Amarillo	\$109.60	\$32.88	1	\$109.60	\$32.88
CBL-50 In unit-out unit Bandabase cable (Ext)	\$67.30	\$24.00	2	\$234.60	\$48.00
Kit de inst. de equipamiento	\$40.00	\$12.00	2	\$80.00	\$24.00
Torre atirantada AT-20 16 mts c/ luz y pararrayos	\$1792.93	\$537.88	1	\$1792.93	\$537.88
Subtotal				\$5300.03	\$1576.63

Tabla 2.5. Costos de Instalación y puesta en marcha

Descripción	Precio CUC	Precio MN	Cant.	Total CUC	Total MN
Inst. de Torre (por día)	\$36.92	\$800.00	2	\$73.84	\$1600.00
Inst. de equipamiento (por día)	\$36.92	\$150.00	2	\$73.84	\$300.00
Programación y puesta a punto (por día)	\$36.92	\$71.40	2	\$73.84	\$142.80
Subtotal				\$221.52	\$2042.80

Total Total CUC: $\$5300.03 + \$221.25 = \$5,521.55$

Total MN: $\$1576.63 + \$2042.80 = \$3,610.43$

2.7 Conclusiones

El detallado estudio de las condiciones del terreno donde se deseó establecer el enlace, Jardín Botánico-FIE, la situación existente en las subredes de ambos sitios, 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 un área universitaria que necesita con urgencia de todos los servicios que se ofrecen para lograr sus objetivos científicos y sociales.

Capítulo III Consideraciones técnicas generales para la puesta en marcha del enlace.

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.

3.1 Sistema de tierra del Jardín Botánico.

La única amenaza natural del equipamiento inalámbrico son los rayos eléctricos. Un rayo puede dañar el equipo con un impacto directo o uno inducido. Los primeros ocurren cuando el rayo realmente alcanza la torre o la antena y el segundo se produce cuando el rayo cae cerca de la torre. Muchos de los métodos utilizados ayudan a prevenir los impactos (Flickenger et al, 2006).

Los sistemas de aterramiento son por lo general una parte integral del sistema de cableado de telecomunicaciones y además de proteger al personal y equipos de voltajes peligrosos, pueden reducir la interferencia electromagnética (EMI) desde y hasta el sistema de cableado de telecomunicaciones, además reducen la posibilidad de inducciones de voltajes que pueden distorsionar o dañar los circuitos de telecomunicaciones. Los aterramientos deberían cumplir con los requerimientos de códigos de las autoridades locales y también deberán alcanzar los requerimientos de ANSI/TIA/EIA.

3.1.2 Proyecto de diseño.

Las redes inalámbricas necesitan de un sistema de aterramiento físico que cumpla con rigor las especificaciones técnicas normadas es por eso que incluimos en esta parte del trabajo el proyecto técnico completo que se implementó en esta área para garantizar la seguridad física de los equipos de radio que allí funcionarán. Estas torres constituyen un pararrayo físico seguro, donde las descargas eléctricas tienen un blanco perfecto para destruir todo el sistema montado, de ahí la necesidad de garantizar el montaje de este sistema con todo el rigor necesario antes de implementar el enlace. Este sistema fue financiado por el Proyecto Belga que tiene este centro.

Generalidades:

El proyecto enmarca el sistema de aterramiento para la protección contra efectos secundarios de las descargas eléctricas atmosféricas y sobretensiones debidas a fallas y/o manipulaciones de la red nacional (SEN), de las redes de datos y equipamiento electrónico a instalar o existente en instalación ubicada en el Jardín Botánico de la UCLV.

El uso de este equipamiento sensible a los procesos transitorios que se inducen en las líneas de alimentación eléctrica, de datos y telefonía requiere del sistema de protección antes citado.

Evaluación de las mediciones realizadas.

Las mediciones para el cálculo de la resistividad del terreno, se realizaron en el área verde posterior al edificio ubicado en el jardín botánico, tal como aparece en el plano de planta en el Anexo XV, garantizándose de esa manera la posibilidad de disponer de espacio para la realización de dicho sistema de aterramiento y para poder contar con la mejor flexibilidad para acceder a la pizarra general de distribución (PGD) principal ó pizarra de distribución del inmueble, lo que permite disminuir al mínimo el potencial en la barra de puesta a tierra en presencia del proceso transitorio.

Método empleado y resultado de las mediciones.

Las mediciones se realizaron con un telurómetro de fabricación Japonesa KYORITSU Modelo 4105, utilizando 3 electrodos dos de ellos como electrodos de alimentación y uno como electrodo de medición.

Los resultados de las mediciones realizadas en el terreno con dicho instrumento, después de promediadas, dieron como resultado una resistencia de puesta tierra del electrodo de prueba de 140Ω .

Calculo del sistema de tierra.

El sistema de tierra se calculó con un programa de computación elaborado en Ecosol Villa Clara, el cual permite el análisis de múltiples variantes y toma en cuenta restricciones del área disponible para acometer el proyecto.

Después de analizar múltiples variantes para este software con el valor medido de resistencia del electrodo de prueba ($140\ \Omega$), se llegó a la conclusión de que la variante más idónea era la solución de la relación longitud separación fuera la de 2 (separación entre electrodos 2 veces la longitud de los mismos), dando un total de 56 electrodos distribuidos en 8 ramas de 7 cada una, pero por las condiciones del terreno que al encontrarse en un área boscosa existen gran número de raíces, las cuales fueron observadas en el momento de realizar las mediciones, el trabajo de excavación de la zanja en una red de tal magnitud se convertiría en algo muy difícil y tedioso conllevando un gran tiempo de ejecución del mismo e incluso el temor de que fuera imposible en algunos sitios, razón por la cual se determinó el uso de electrodos de grafito los cuales su ubicación es más puntual y ocupa un área muchísimo menor que para el caso de una malla con electrodos convencionales. La forma de montaje e instalación se muestra en los planos del Anexo XVI. Como resultado de la valoración según características del terreno medido para lograr una resistencia de puesta a tierra de $0.5\ \Omega$ se proponen 3 electrodos de grafito, una vez comprobada que la diferencia de potencial entre los diferentes puntos del terreno donde se implementará el sistema de aterramiento es cero.

Para la conexión a tierra física del bajante de la punta Franklyn (punta pasiva) a ubicar en la torre de radio enlace como protección para la misma, se implementará una puesta a tierra conformada por 3 electrodos convencionales dispuestos en triángulo, la longitud de los electrodos será de 1.5m y la separación entre los mismos será de 3m, el conductor de enlace será de cable de cobre desnudo de sección 50mm^2 enterrado a una profundidad de al menos 0.5m, este sistema de puesta a tierra al cual se conectará la torre tendrá un valor máximo de $10\ \Omega$. Se dejará en muro un desconector mecánico para la conexión del bajante de la antena.

Ambos sistemas se unirán físicamente, el sistema de puesta a tierra (SPT) para la protección y funcionamiento del equipamiento sensible que requiere de $0.5\ \Omega$ y el SPT para la antena ante el posible impacto directo de una descarga, conformando un sistema equipotencial y único de protección.

La pizarra general de distribución de entrada a la instalación que se muestra en la figura del Anexo XVII, presenta dos niveles de supresión y además presenta las respectivas

bobinas de desacople para garantizar que los supresores de cabecera y los de segundo nivel coordinen para garantizar la operación segura de los mismos. Los supresores de cabecera son de 100kA, producto a que existe un pararrayos ubicado en la torre de la conexión inalámbrica lo que hace posible que la radiación electromagnética pueda ser de un valor considerable. Después de ejecutado el proyecto se hace la certificación del mismo a la Empresa APCI que es la que se encarga de dar la calidad final del sistema.

Existen varias normas que rigen estos sistemas que pueden ser consultadas en la referencia (Cuba. Oficina Nacional de Normalización, 2006a) y (Cuba. Oficina Nacional de Normalización, 2006b).

3.2 Utilitario de administración para el KBEST

En la Empresa de Construcción y Mantenimiento para la Industria Eléctrica (ECIE) existe un enlace de radio que une la dirección de esta empresa con el despacho de carga y que esta aproximadamente a 4 Km. de distancia entre los dos puntos. Este enlace usa equipos de la firma KBEST que es el mismo que se usará para el enlace entre el Jardín Botánico y la Facultad de Eléctrica y fue el tomado como referencia para la parte practica-administrativa del enlace.

El equipo KBEST tiene dos formas de administrarse una es por WEB y la otra forma es usando un utilitario que se nombra Wireless Smart Utility y se instala en la maquina desde donde se administra el equipo. Cada uno tiene un ambiente diferente pero da las mismas posibilidades de configuración. A continuación de forma detallada se explican cada una de las opciones de administración y configuración que ofrece. (802.11g Outdoor Bridge Hotspot, 2004). (ZyXel, 2005)

La primera pantalla que se muestra cuando se ejecuta este utilitario es un buscador que detecta todos los equipos inalámbricos que están conectados a la red que sean de la firma Best-Link (Figura 3.1). En este caso solo se muestra el punto de acceso y la estación cliente porque es un enlace punto a punto. Queda como sigue:

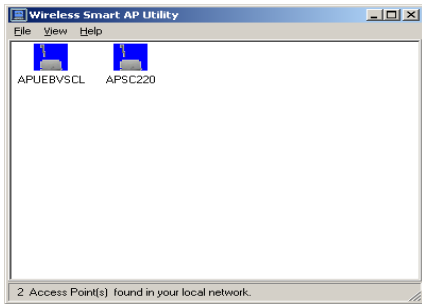


Figura 3.1. Búsqueda.

Al dar doble clic sobre uno de los equipos se pide la contraseña de acceso que debe ser cambiada la primera vez que acceda, pues vienen con una contraseña por defecto igual para todos los equipos que vende la firma que sean de la misma serie. La figura 3.2 muestra la información general del equipo seleccionado. La dirección MAC única que lo identifica, la versión de Firmware que tiene instalada, la versión del Boot, y la versión del utilitario de administración.

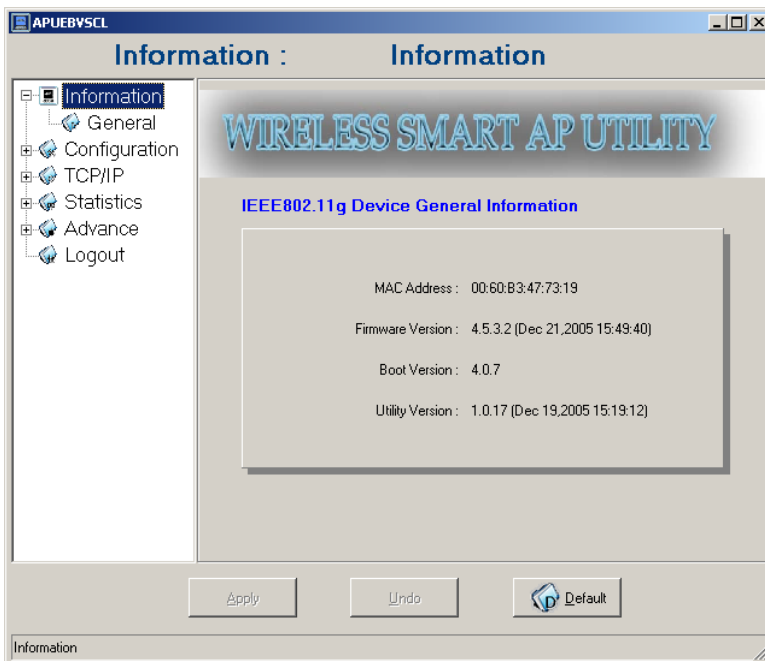


Figura 3.2. Información general del equipo

En la pantalla que sigue (Figura 3.3) comienza ya la configuración de todos los parámetros generales del equipo. Se adicionan por parte del administrador los siguientes datos:

Nombre del Punto de Acceso que se desea. En este caso se nombra APUEBVCL y la estación cliente APSC220.

Modo inalámbrico: Puede ser como Punto de Acceso o como Estación. En el caso de Estación debemos especificar el tipo de topología de red que se usara. Puede ser Ad-Hoc o Infraestructura.

ESSID: Es el identificador de Red. Es único para el enlace.

Modo: Define el tipo de enlace según la norma IEEE 802.11. En este caso esta G, B, o B y G mezclados.

Rate o Velocidad del enlace: Se usa para fijar la velocidad del enlace. Normalmente en Auto para que el sistema decida la velocidad según las condiciones que existan en cada momento.

País o Región: Están incluidos los países que tienen canales de frecuencia asignados por los organismos internacionales.

Canal de frecuencia: Cada país que tenga permisos internacionales para usar las redes inalámbricas tiene un rango de canales de frecuencia dentro de la banda de frecuencia en que opera el equipo de radio que use. En Cuba el organismo rector es la Agencia de Supervisión y Control del Ministerio de Comunicaciones (MIC). Para el enlace tomado como caso de estudio se configurado el canal 1 que esta en la frecuencia de 2,412 Ghz.

El punto de acceso lo configuramos como modo AP, el identificador de red como ECIE, para la norma IEEE 802.11g, el país USA que es el tiene asignados canales de frecuencia según las normas internacionales y escogemos el canal 1.

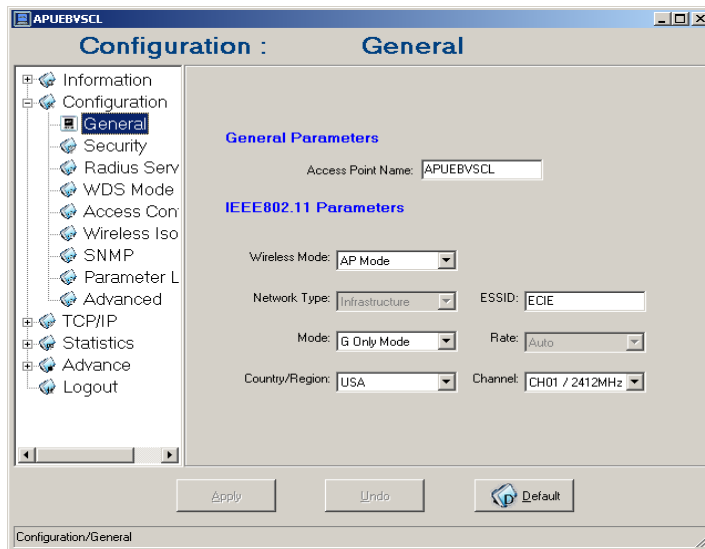


Figura 3.3. Configuración general.

Seguidamente la figura 3.4 muestra las opciones de configuración para la seguridad del enlace según la norma IEEE 802.11i y IEEE 802.11x que contempla cinco niveles de seguridad usando los diferentes protocolos de encriptación de la información y que se ordenan como sigue:

Tipos de encriptación: Open Auto, Shared Key, 802.1x, WPA-PSK, WPA.

Open(Auto): Es la autenticación por defecto, no requiere de ningún chequeo de seguridad para unir usuarios a la red, se dice que el sistema esta abierto.

Shared Key: Esta opción nos permite poner una llave compartida que será la misma para el punto de acceso y la estación conectada a él.

Las demás variantes se configuran aproximadamente de la misma manera, permitiendo introducir una llave o una clave primaria, pero el de mayor seguridad es el WPA-PSK que es la combinación de WPA con una llave precompartida. En este enlace se usa el protocolo WPA-PSK con la opción TKIP donde cada usuario tiene su propia clave de encriptación y puede ser establecida de modo que cambie periódicamente. Es importante señalar que cuando el AP esta configurado como estación no están disponibles los modos WPA y 802.1x.

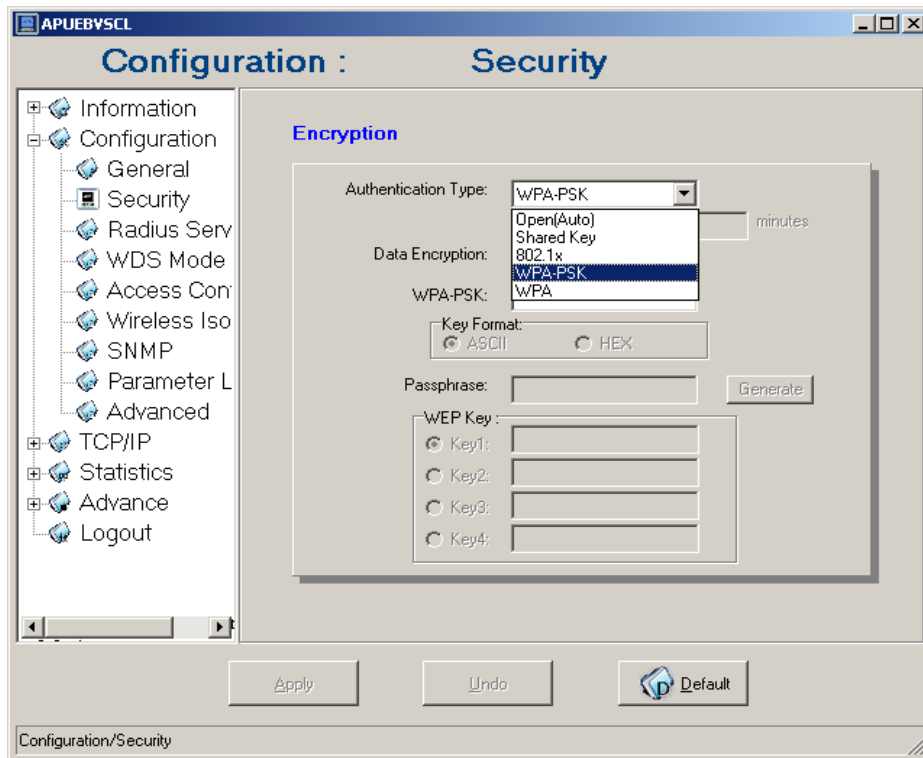


Figura3.4. Seguridad.

La figura 3.5 es para usar un servidor Radius instalado en un servidor remoto (Linux o Windows) y es en esta pantalla donde se le dice al equipo de radio cuales son los datos de este servidor para que sea administrado desde el. Es la opción más segura cuando se trata de la autenticación de los usuarios. Los detalles teóricos aparecen en el epígrafe 1.12. Para usar esta variante es necesario tener habilitados los protocolos WPA y 802.1x en la ventana de configuración de la seguridad. En nuestro caso esta opción está deshabilitada pues como los equipos de radio solo se usan como puntos de acceso para unir dos redes cableadas no es necesario usar servidores de autenticación de usuarios.

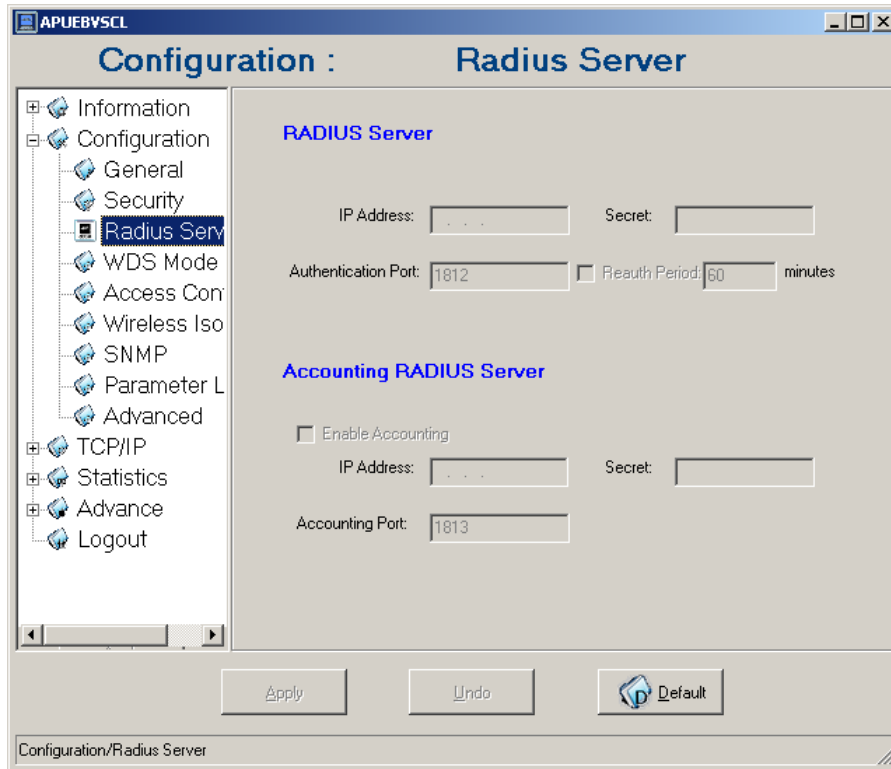


Figura 3.5 Servidor Radius.

El Modo WDS se usa cuando tenemos dos equipos que están siendo usados como puntos de acceso para diferentes estaciones y se necesita unirlos haciendo un enlace entre ellos, así se aprovecha la posibilidad de brindar servicio inalámbrico en ambos equipos. En este enlace esta opción esta deshabilitada.

Tiene tres variantes de configuración:

Deshabilitado: No permite enlaces WDS.

Auto WDS: Cualquier AP puede conectarse a nuestro AP

Manual: Se especifica cuales son las direcciones MACs del AP con el que se va a enlazar en modo WDS. Se pueden hacer cuatro enlaces entre puntos de acceso. Para el enlace tomado como ejemplo esta opción esta deshabilitada. (Figura 3.6)

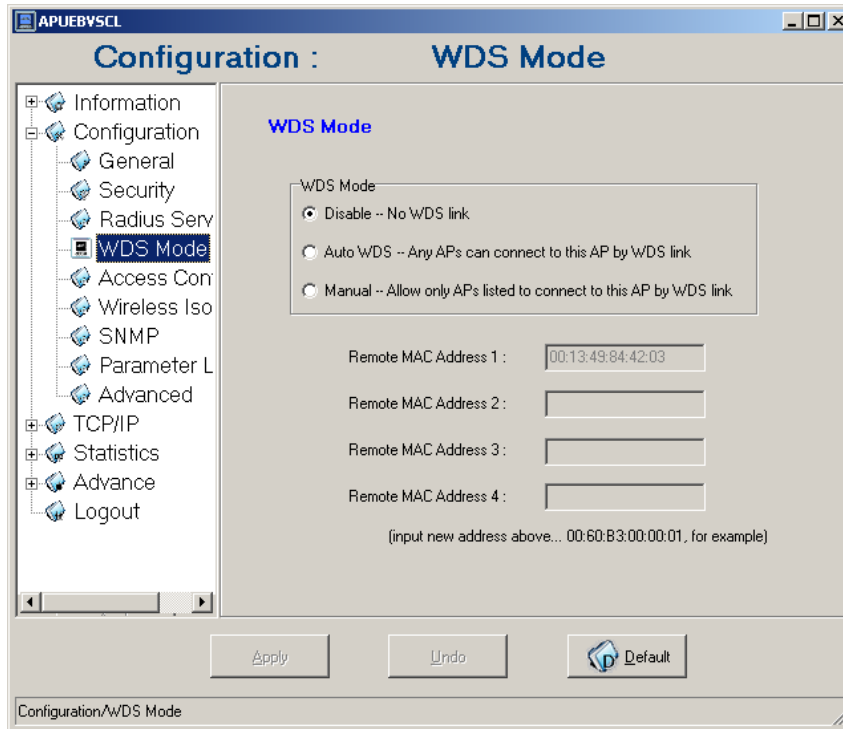


Figura 3.6. Modo WDS.

El Control de acceso (figura 3.7), es otra de las variantes que usa el equipo de radios para garantizar la seguridad en los enlaces inalámbricos y nos permite tres maneras posibles de configuración:

Open: Abierto a todos los usuarios que deseen conectarse.

Allow: Permite el acceso de los dispositivos cuya dirección MAC este en la lista de acceso.

Deny: Deniega el acceso de los dispositivos cuya MAC este en la lista de acceso.

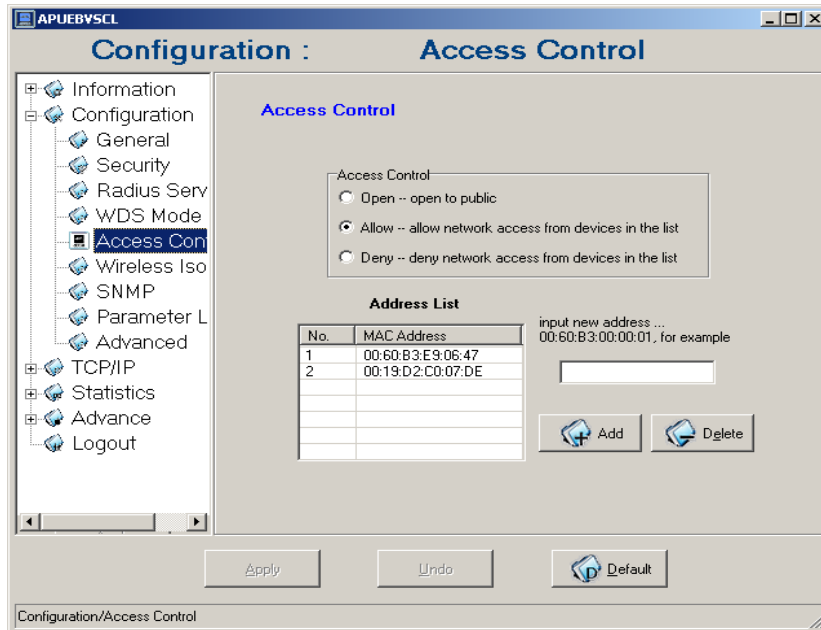


Figura 3.7.Control de acceso.

Para lograr mayor seguridad escogemos la opción Allow que permite acceder al AP solo a los dispositivos cuyas direcciones MAC aparecen en la lista, fuera de eso ningún otro se puede conectar.

El Aislamiento inalámbrico (Wireless Isolation) se configura para que los equipos de radio se aíslen o no del área de servicio. La figura 3.8 muestra las diferentes formas de configuración.

Disable Isolation (Aislamiento deshabilitado): Todas las estaciones pueden comunicarse entre si. Es la opción por defecto.

Complete Isolation (Aislamiento completo): Ninguna estación puede comunicarse entre si.

Group Isolation (Aislamiento por grupo): Solo se permite la comunicación entre las estaciones que pertenecen a un mismo grupo. Se pueden crear hasta cuatro grupos. En este equipo se crea un solo grupo pues solamente hay dos AP enlazados y se le adicionan las direcciones MAC de las estaciones que se pueden comunicar entre si.

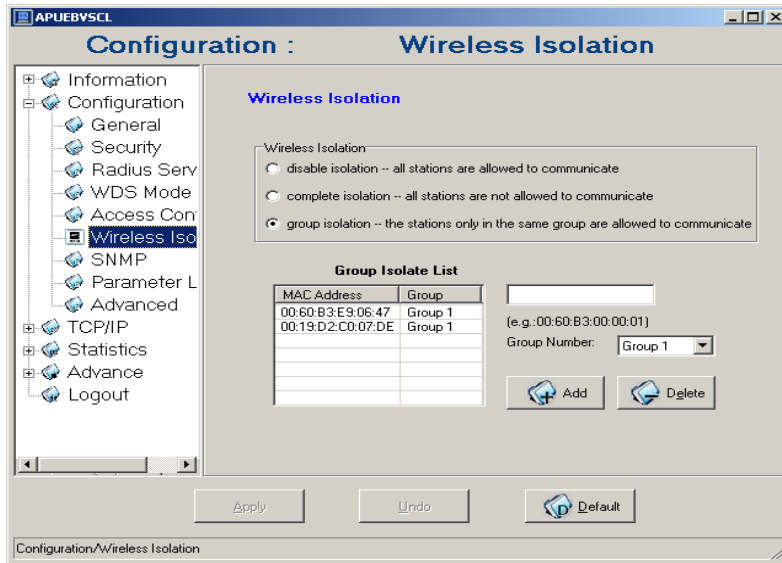


Figura 3.8. Aislamiento inalámbrico.

El equipo permite ser administrado usando el protocolo SNMP (Figura 3.9), para monitorear el tráfico en la red. Para habilitar el servicio es necesario que el equipo conozca cual es la dirección IP del servidor SNMP, la comunidad de solo lectura que usualmente se nombra como public y es para que los usuarios puedan solamente ver las graficas de trafico y la variante Read-Write Community que le permite al administrador del SNMP leer y escribir los MIB (Management Information Base) que genera el equipo de radio. Este protocolo esta habilitado y mas adelante en el epigrafe de monitoreo y gestión del enlace se dan los detalles de configuración.

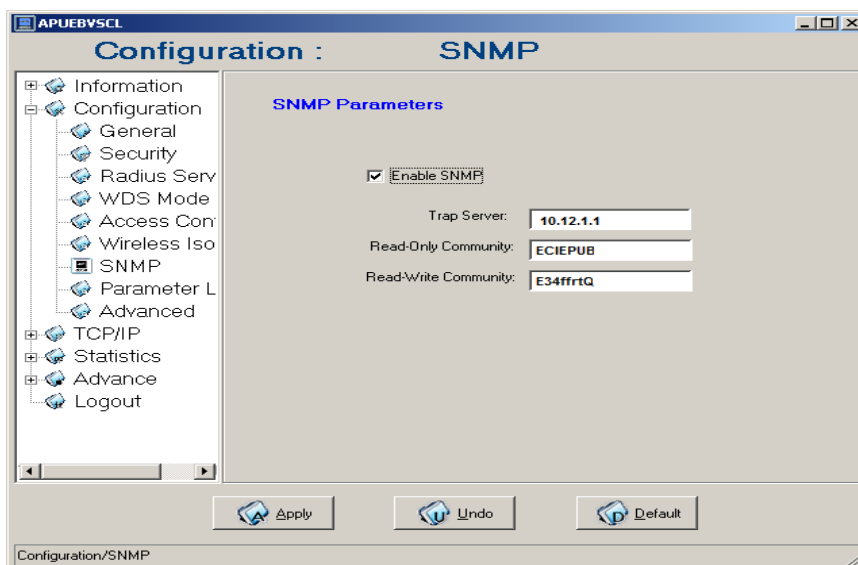


Figura 3.9. Protocolo SNMP.

La pantalla de Parameter log nos permite guardar en un archivo de una PC que pertenezca la red la configuración que tiene el equipo así como restaurar la configuración en el momento que se desee. Figura 3.10.

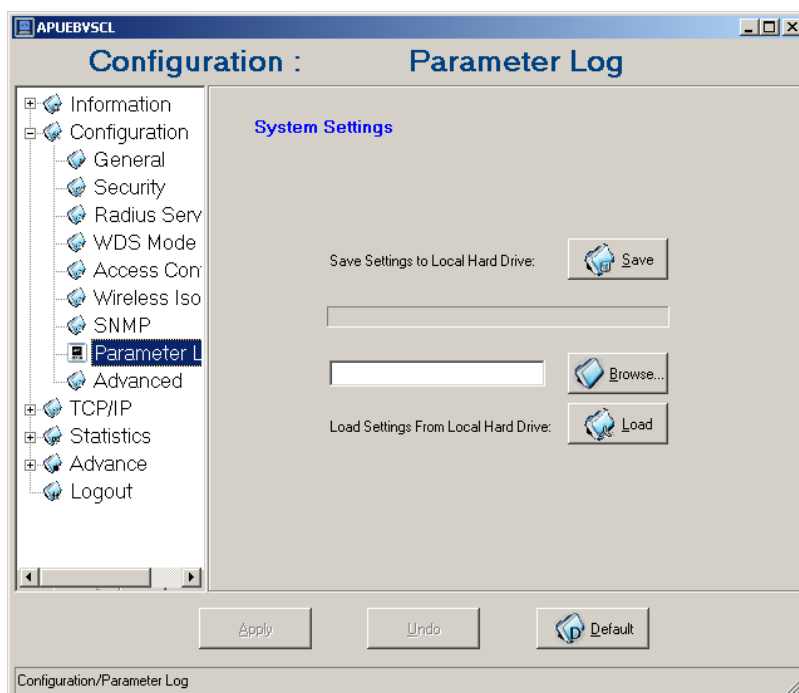


Figura 3.10. Parameter log.

Entre los parámetros avanzados tenemos:

RTS Threshold: Es un mecanismo implementado para prevenir el “Nodo oculto”. Si el tamaño del paquete transmitido es mayor que el valor que se configuró se habilita el RTS y la comunicación entre el punto de acceso y la estación usa RTS/CTS para la transmisión de datos. El rango de configuración que admite es de 0-2347.

Frag Threshold: Es un mecanismo de fragmentación que se usa para mejorar la eficiencia cuando existe un alto tráfico en la red inalámbrica para mejorar la transferencia de ficheros grandes a través de la red. El rango de configuración está entre 256 y 2346. Por ejemplo si se pone el valor de 256 significa que el paquete puede ser fragmentado en 256 bytes cuando se está transmitiendo.

DTIM: Este valor es el mensaje de indicación del tráfico enviado. (Delivery Traffic Indication Message).

Beacon Interval: Es un paquete de transmisión que mantiene a la red sincronizada.

Preamble: Define el tamaño del campo de sincronización PLCP (Protocolo de convergencia del nivel físico) para la comunicación entre el punto de acceso y la tarjeta de red. La opción por defecto es Auto.

Enable Protection: Si esta habilitada el sistema envía un paquete RTS/CTS desde el equipo de radio.

Ocultar el AP: Disponible solo para el modo AP y el aislamiento inalámbrico. Se usa para ocultar el punto de acceso, y es necesario que la estación conozca el identificador ESSID del AP a donde se conectará. Los valores que tiene configurado el enlace se muestran en la figura 3.11:

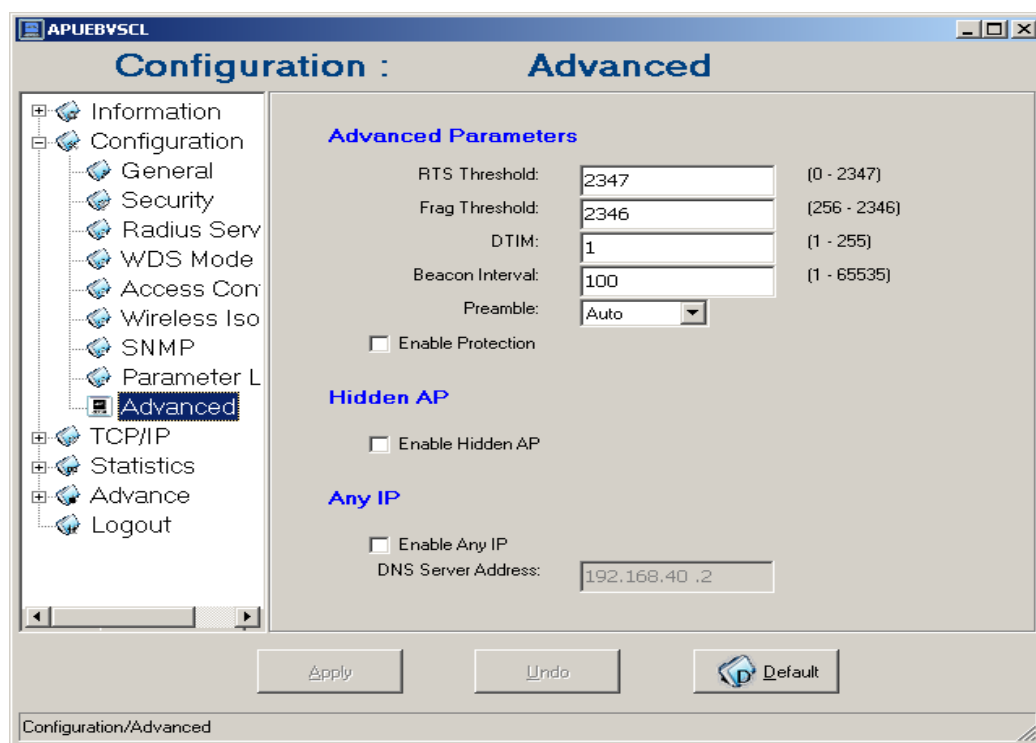


Figura 3.11. Configuración avanzada.

Configuración de los parámetros para el protocolo TCP/IP. Ver figura 3.12.

Figura 3.13. Estadísticas generales.

Estadísticas para el punto de acceso (AP Browser, Buscador de puntos de acceso). Disponible solo para el modo estación. El AP Browser (Figura 3.14) muestra la lista de puntos de acceso disponibles para conectarse, eligiendo con cual se desea la conexión.

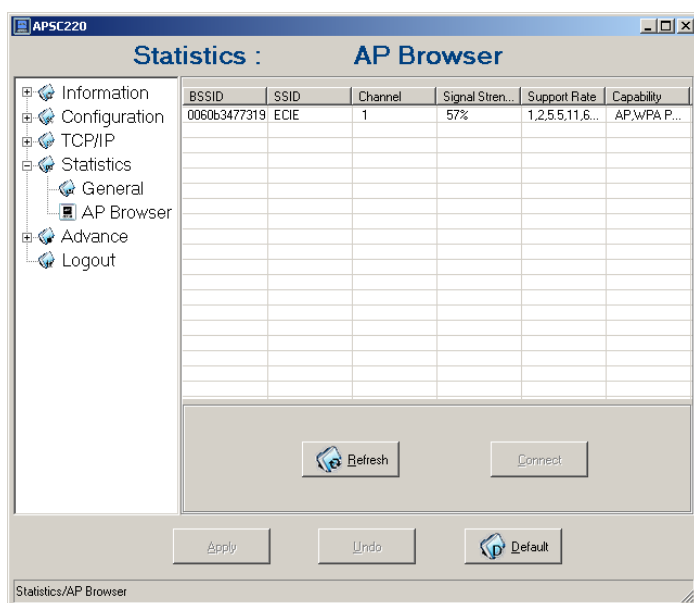


Figura 3.14.AP Browser.

Opciones avanzadas. Actualización del Firmware del equipo según la norma 802.11 para redes WLAN.

Estos equipos tienen una clave para la administración de sus parámetros por defecto (default) que es necesario cambiar en cuanto comience su explotación para garantizar la privacidad administrativa del AP. Ver figura 3.15.

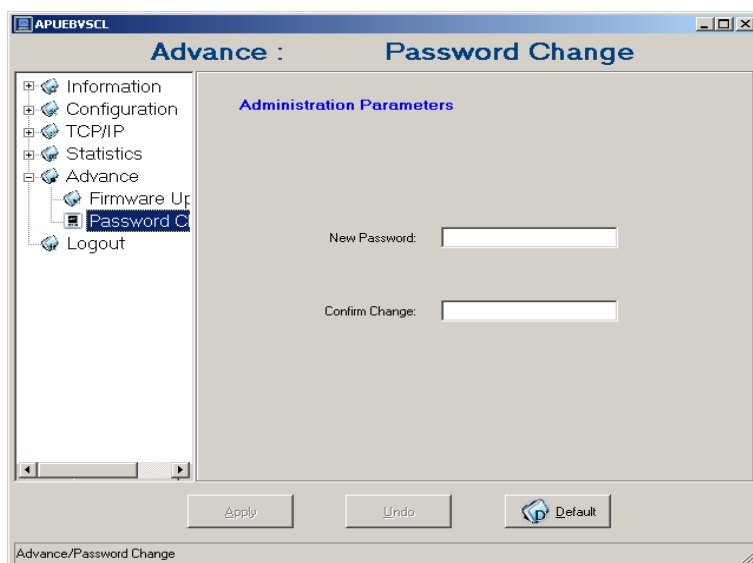


Figura 3.15.Cambio de contraseña de administración.

Y por ultimo queda cerrar la sesión de administración (*logout*) que debe hacerse cada ves que el administrador del enlace acceda al programa de administración pues si se cierra la ventana sin dar el cierre de sesión puede suceder que este software no funcione apropiadamente cuando vuelva a ser ejecutado y no sea capaz de encontrar los equipos de radio en la red. Para resolver esto es necesario apagar y encender el equipo desde el lugar donde esta alimentado en el gabinete de conexiones. Figura 3.16.

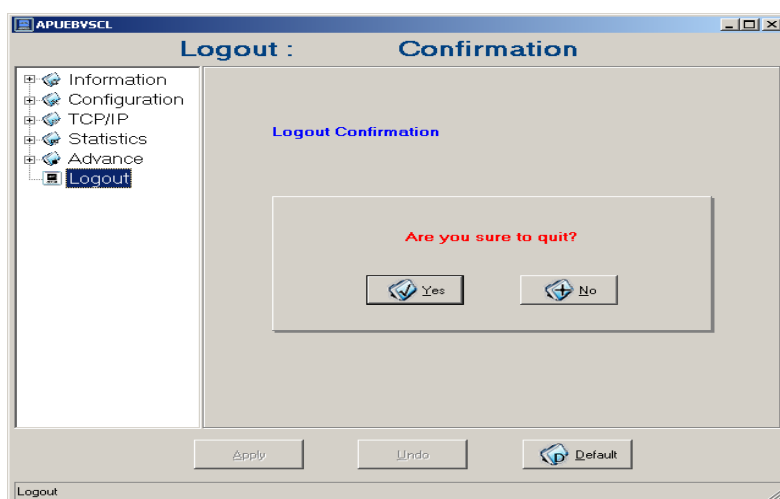


Figura 3.16.Cerrar la sesión de administración.

El sitio WEB para la administración remota de los equipos de radio tiene las mismas opciones generales y de configuración. La diferencia esta en el ambiente que muestra la

página. Se puede acceder usando la dirección IP de la maquina (para la aplicación objeto de estudio en esta tesis: [http:// 192.168.40.35](http://192.168.40.35)) o por DNS (primero debe estar creado el record en el servidor de dominio) usando el nombre del equipo (para nuestro caso de estudio: <http://apuebvcl>). A continuación (Figuras 3.17 y 3.18) se muestran dos de las páginas más representativas de este sitio que es suministrado por el vendedor.

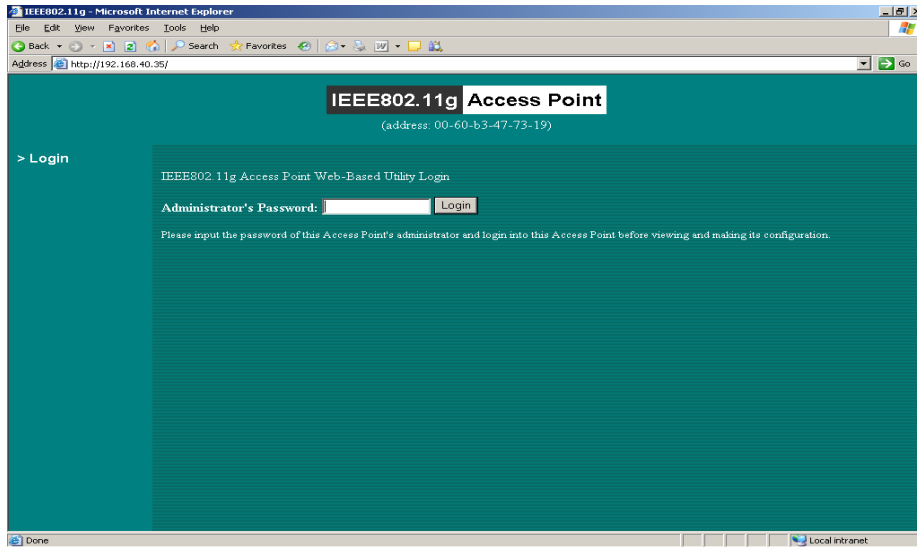


Figura 3.17 Página de acceso al administrador WEB del equipo de radio KBEST.

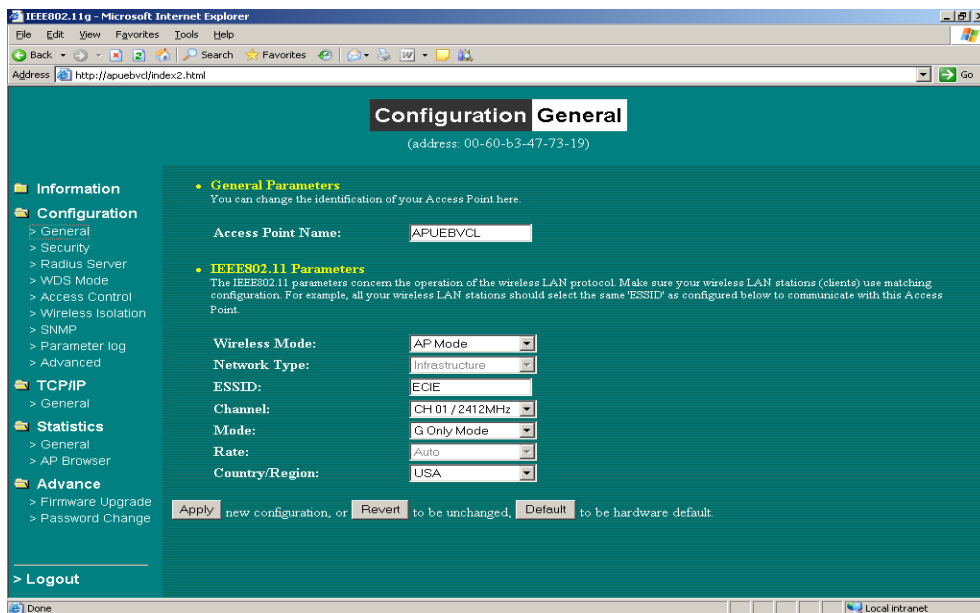


Figura 3.17 Página de acceso a la configuración general por WEB del equipo de radio KBEST.

3.3 Monitoreo y Gestión del Enlace.

Para comprender los resultados del monitoreo del enlace es necesario recordar algunos conceptos analizados anteriormente.

El más importante de los valores, la velocidad máxima alcanzada depende inversamente de la distancia de los equipos y varía por variables que no son controlables por los encargados del enlace como por ejemplo el estado ambiental. Ver Anexo XVIII

En la figura 3.19 se puede ver que el parámetro “Signal Strength” está en un 55%. Poco después el valor se desplazo a 52% donde osciló por varios minutos. Los valores máximos a los que llega el enlace están alrededor del 63% de la velocidad máxima para el equipo de radio KBest.

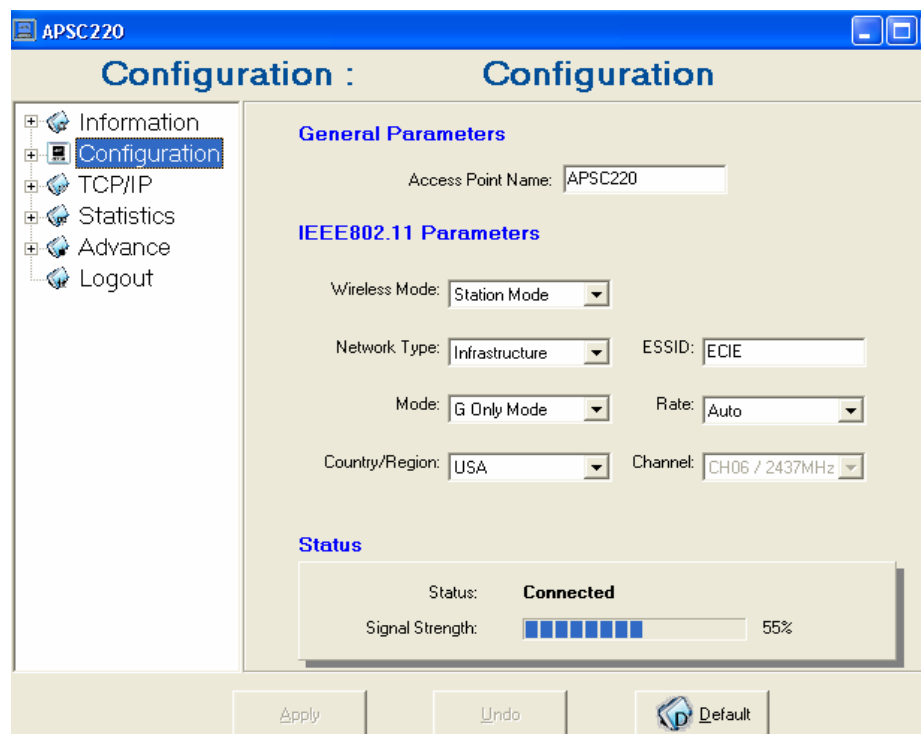


Figura 3.19 Velocidad de ocupación del canal.

Este dispositivo como la mayoría de los equipos para redes soporta los estándares de gestión y supervisión que existen en el mercado.

En la figura 3.20 se muestra el panel de configuración de SNMP.

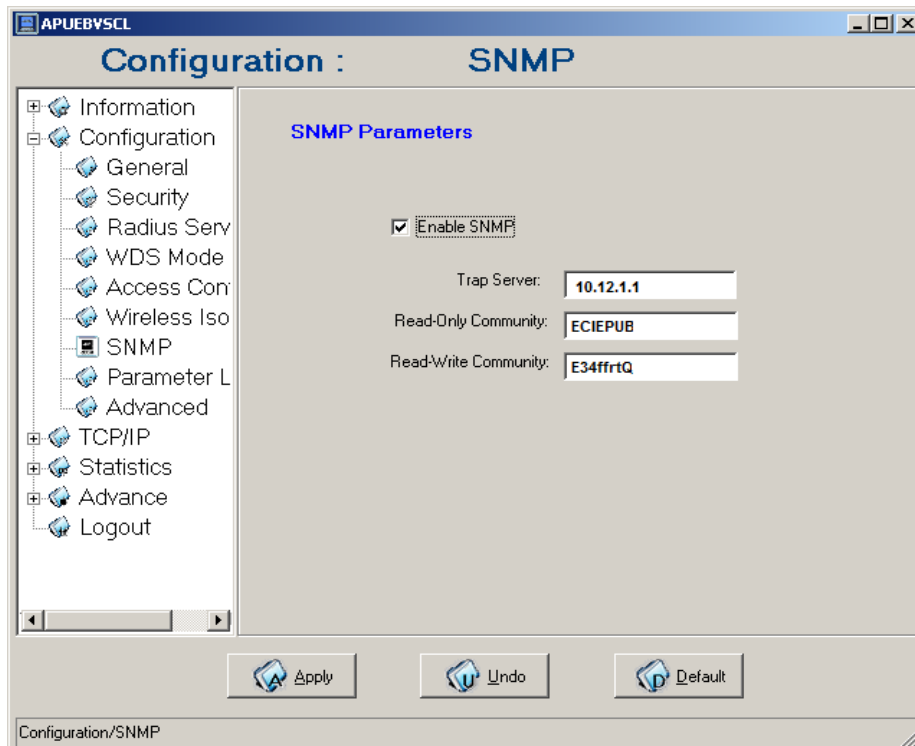


Figura 3.20 SNMP

El uso de SNMP permite la supervisión en tiempo real de los parámetros de trabajo del equipo y la creación de gráficos de tráfico. Estos gráficos se realizan generalmente con programas que generan páginas web permitiendo así el acceso desde lugares muy diferentes. En el caso que se analiza se escogió el CACTI como programa de gestión y los gráficos de “Bytes IN” y “Bytes OUT” contra tiempo. Una gráfica de este sistema se muestra en la figura 3.21

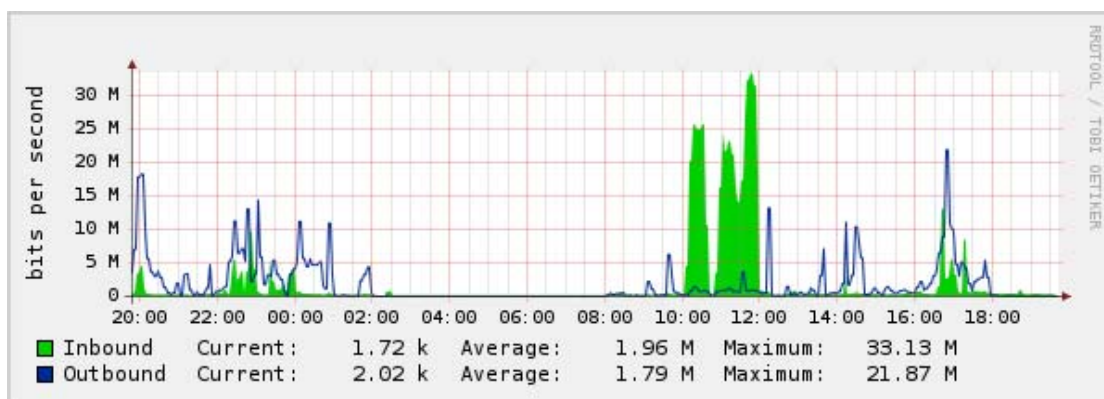


Figura 3.21

Como se puede ver la máxima velocidad alcanzada no llega a los 54 Mbits. Esto se debe a la distancia entre los puntos y el tipo de modulación usada.

En el anexo XIII se puede ver la relación entre la velocidad y los diferentes esquemas de modulación que pueden ser usados.

Si aplicamos esto al caso universitario con el equipo de radio Kbest, en el enlace entre el Jardín Botánico y la Facultad de Ingeniería Eléctrica se puede decir que este enlace funcionará a velocidades cercanas a los 54 Mbps si se usa 64QAM como esquema de modulación porque la distancia entre ambos lugares es poco mayor que 500 m.

3.5 Soluciones alternativas de respaldo ante situaciones que comprometen la continuidad de los servicios de la red.

La UCLV pretende emplear la tecnología inalámbrica en todo su campus universitario como método de respaldo ante cualquier situación de contingencia que pueda sustituir los enlaces actuales con fibra óptica para lograr la redundancia de la red UCLV y también crear zonas WI-FI que cubran las principales áreas universitarias donde los usuarios puedan acceder a la red con la utilización de una tarjeta inalámbrica, válido para salones de reuniones, áreas de descanso, salones de estudio y otros. El enlace entre el Botánico y la FIE puede ser usado como parte de este proyecto extensible pues los puntos de acceso que se han comprado pueden, además de dar servicio al enlace, ser usados para cubrir algunas zonas universitarias incorporándole las antenas necesarias, por la ubicación geográfica que tienen los dos lugares donde se montarán.

3.6 Conclusiones

El equipo de radio Kbest que usa el enlace inalámbrico diseñado es fácil de administrar y configurar y puede usarse para diferentes tipos de enlaces pues cumple con los requerimientos técnicos que plantean las normas IEEE 802.11g y 802.11x. Se logra una estabilidad máxima en el enlace y si las condiciones climáticas no son buenas solo disminuye la velocidad a la que se logran conectar ambos equipos pero no se cae el enlace. La velocidad de transferencia de ficheros no es muy alta solo necesitamos un tiempo mas largo pero lo mas importante de los enlaces inalámbricos es la posibilidad que tienen de

unir áreas de difícil acceso a las redes de cables lo que justifica completamente las bajas velocidades comparadas con las del orden de Gb que se alcanzan en las redes LAN cableadas.

CONCLUSIONES

1. Las redes de área local inalámbricas constituyen una alternativa a las redes cableadas y permiten la comunicación mediante ondas de radio.
2. Existen numerosos estándares IEEE 802.11 que responden a diferentes aplicaciones, entre los que se destacan: IEEE 802.11a, IEEE 802.11b y IEEE 802.11g.
3. El análisis de las características de un radioenlace tales como pérdidas básicas de propagación, la sensibilidad en el receptor, los niveles de potencia transmitida, resultan de suma importancia para el diseño de un enlace.
4. 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.
5. Se realizó el diseño teórico de una red de área local inalámbrica para interconectar el Centro de Investigación del Jardín Botánico con la FIE.
6. Se hizo el proyecto técnico y el montaje del sistema de aterramiento del Jardín Botánico según los requerimientos del terreno y las normas nacionales vigentes.
7. Se comprobó en el enlace que funciona en la ECIE que si el equipo de radio esta bien configurado esta garantizada la seguridad del enlace.
8. La velocidad de los enlaces inalámbricos pueden variar debido a condiciones ambientales y de la distancia entre las antenas transmisora y receptora.

RECOMENDACIONES

Este trabajo llega hasta del diseño teórico del enlace aunque se describe la manera en que puede ser administrado y configurado y se hacen estudios de tráfico y ocupación del canal. Queda entonces la terminación del montaje del equipamiento, la configuración y puesta en marcha del enlace tomando como base todo el estudio y las pruebas practicas que se hicieron con la ECIE.

Este trabajo se hará de Conjunto con Copextel y el Grupo Central de Redes de la Universidad. Por lo que se proponen las siguientes recomendaciones:

1. Aplicar el diseño teórico al montaje del enlace y las experiencias practicas de administración que se dan en el capítulo 3 para la configuración y rendimiento de la subred que allí se creará.
2. Realizar un estudio y proponer un proyecto para usar este enlace en la interconexión de otras zonas de la Universidad.
3. Utilizar las WLAN para lograr la redundancia de la red universitaria y en el caso que existan fallas, no se afecten los servicios.

REFERENCIAS BIBLIOGRÁFICAS

802.11g Outdoor Bridge Hotspot (2004). User's Manual

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 2 de mayo de 2007]

Álvarez Calvo, M. et al. (2005) "Las Telecomunicaciones y la Movilidad en la Sociedad de la Información" en *TID Telefónica I+D*. [En línea]. España, disponible en: http://www.tid.es/html/libros_sector_telecomunicaciones.html0.pdf [Accesado el día 22 de marzo de 2007]

Andueza Unanua, Angel M. (2003). Redes de Acceso de Banda Ancha en Navarra. [En línea]. España. Disponible en: <http://www.unavarra.es/organiza/etsiit/cas/estudiantes/pfc/redacna/Tecnologias%20de%20Acceso/WLAN/elementos%20red/acceso%20al%20medio.htm> [Accesado el día 15-marzo-07]

Bates, Regis., (2003) *Comunicaciones inalámbricas de banda ancha*. Mc Graw-Hill/Interamericana de España. Madrid. España.

Breeze Access TM II. (2004) en *Alvarion*. [En línea]. Disponible en: www.owns.bfioptilas.es/html/rf_mw/access_vl.pdf [Accesado el día 27 de abril de 2007]

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 5 de abril de 2007]

Calderón, O. y V. Quintero, (2004) "Un nuevo aspecto de la movilidad: redes Ad-Hoc-conceptos" en *Revista Colombiana de Tecnologías de Avanzada*. Volumen 1 No. 3. 2004, Facultad de Ingeniería Electrónica, Universidad de Cauca. [En Línea]. Disponible en: <http://www.control-automatico.net/PDF/Revista%203/redes.pdf> [Accesado el día 31 de mayo de 2007]

- Carlson, B. Paul, C. y J. Rutledge, (2002) *Communication Systems, an introduction to signals and noise in electrical communication*. 4a edición, Mc Graw-Hill, Nueva York, EUA.
- Cors, I; Pernich, P. (2004). Seguridad en redes wireless.
- Cuba. Oficina Nacional de Normalización (2006a) NC IEC 62305-1: 2006, IDT. Protección contra rayos – Parte 1: principios generales. 1.ed. La Habana, NC.
- Cuba. Oficina Nacional de Normalización (2006b) NC IEC 6332-2: 2006, IDT. Protección contra rayos – Parte 2: gestión de riesgos. 1.ed. La Habana, NC
- DLink Latinoamérica. (2004) “Redes inalámbricas” en *Maestros del Web*. [En línea]. Disponible en: <http://www.maestrosdelweb.com/editorial/redeswlan/> [Accesado el día 2 de marzo de 2007]
- Earte, A. (2006). *Wireless Security handbook*. Boca Raton, FL, Taylor & Francis Group, LLC
- Fernández G. E., (2007) “Wi-Fi: nuevos estándares en evolución” en *Centro de Difusión de Tecnologías CEDITEC ETSIT-UPM*. Universidad Politécnica de Madrid. [En línea] España, disponible en: <http://www.ceditec.etsit.upm.es/InfTecnologia/wifi.pdf> [Accesado el día 26 de febrero de 2007]
- 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/mon04.pdf [Accesado el día 30 de febrero de 2006]
- Flickenger, Rob.; et al. (2006) “Redes Inalámbricas en los Países en Desarrollo Una guía práctica para planificar y construir infraestructuras de telecomunicaciones de bajo costo” en *Montevideo Libre*. [En línea]. Disponible en <http://www.montevideolibre.org/doku.php/manuales:libros> [Accesado el día 17 de abril de 2007]
- Fout, T. Barkley, W. Y M. Lee. (2007) “Tecnologías de redes inalámbricas y Windows XP” en *Latinoamerica Microsoft TechNet*. Disponible en

<http://www.microsoft.com/latam/technet/articulos/windowsxp/2008/default.asp>

[Accesado el día 20 de febrero de 2007]

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 17 de mayo de 2007]

Geier, Jim. (2002) “802.11a: An Excellent Long Term Solution” en *Wi-fi planet*. Disponible en: <http://www.wi-fiplanet.com/tutorials/article.php/1436331> [Accesado el día 11 de abril de 2007]

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

Introducción a la Tecnología Wireless 802.11 en *Advento networks*. [En línea]. Disponible en: http://www.e-advento.com/tecnologia/wlan_intro.php [Accedido el día 1 de junio de 2007]

K-BEST Tech Wlan Solutions (2005) Official Product Catalogue en *K-Best technology*. [En línea]. Disponible en: http://www.electronics.intron.hu/katalogus/INTRON_K-Best_KAT_Ang.pdf [Accesado el día 12-marzo de 2007]

Kreft, A. (2003) “Redes Inalámbricas” en *pc-news.com*. Estados Unidos, disponible en: <http://www.pc-news.com/detalle.asp?sid=&id=4&Ida=1270> [Accesado el 1 de mayo de 2007]

León-García, A., e I. Widjaja, (2005) “*Communications Networks. Fundamentals Concepts and Key Architecture*”. Mc Graw-Hill, Nueva York, EUA

Leyva, E., (2005). “ Qué es Wi-Fi? Algunas aplicaciones”. *Tono*. Número 3, 2005, pp. 12-15.

Luther J., (2005). “Una guía de los estándares inalámbricos. El alfabeto 802.11 en *Linux Magazine*. No. 4. 2005. [En línea]. España, disponible en: <https://www.linux-magazine.es/issue/04/80211.pdf> [Accesado el día 12 de marzo de 2007]

- Martínez, E. y J. A. García. (2006). “Redes Wi-Fi en malla (wi-fi mesh networks)” en *Eveliux.com-Tecnologías de información*. [En línea]. México, disponible en: <http://www.eveliux.com/index.php?option=content&task=view&id=92&Itemid=> [Accesado el día 30 de mayo de 2007]
- Matos, J.; (2005) *TV Directa por satélite*. España.
- MicroAlcarria, (2007). Cálculos para realizar un enlace wireless en *MicroAlcarria*. [En línea]. Disponible en: http://www.microalcarria.com/miscelanea/calculos_enlace_wireless/ [Accesado el día 12 de abril de 2007]
- Novakovic, Z.; (2004) “Roaming and WLAN” en *MobileIN.com*. [En línea]. Disponible en: http://www.mobilein.com/Perspectives/Authors/zagaWLAN_Roaming.htm [Accesado el día 9-mayo-07]
- Paramowifix, (2007) “Link Planning for Wireless LAN (WLAN)”. [En línea]. Disponible en: <http://www.paramowifix.net/antenas/calculoenlacewlan.html> [Accesado 12 de abril de 2007]
- Proakis, J., (2001) *Digital Communications*. Tomo 3, 4ta Edición, Nueva York, Mc Graw-Hill, EUA.
- Proyecto Extremadura. (2007) “Redes Inalambricas. Antenas” en *Wepcc*. [En línea]. Disponible en: http://rinuex.unex.es/modules.php_38_antennas [Accesado el día 19 de abril de 07]
- Ramasarma, V., (2002) “A Coverage Area Estimation Model for Interference-Limited Non-Line-of-Sight Point-to-Multipoint Fixed Broadband Wireless Communication Systems”. Trabajo de Máster en Ciencias. Instituto Politécnico de Virginia. EUA.
- 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 29 de abril de 2007]
- Sklar, B., (1998) *Digital Communications. Fundamentals and applications*. Tomo 2, Nueva Jersey, Prentice Hall, EUA.

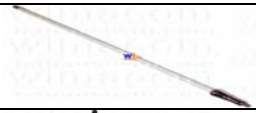





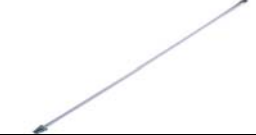

- Sotolongo Gómez, A. y T. Poveda Bestard, (2006). “Modulación por conmutación de código complementario” en *Telem@tica* Año IV No. 5. Enero 2006, Departamento de Telemática del Instituto Superior Politécnico José Antonio Echeverría. [En línea]. Cuba. Disponible en: http://www.cujae.edu.cu/revistas/telematica/Publicaciones/Telem@tica_AnoIV_No15.pdf [Accesado el día 30 de marzo de 2007]
- Tienda de Productos Inalámbricos (2007). En Wimaxcom Instalaciones Wi-Wireless. [En línea]. Disponible en: <http://www.wimaxcom.com/tienda/> [Accedido 17 de mayo de 2007]
- Tsunami Quickbridge Wireless Radio Outdoor (2002) en *Proxim*. [En línea]. Disponible en: www.nationalwireless.ie/pdfs/quickbridge20_a4.pdf [Accesado el día 24 de febrero de 2007]
- Wang, X. y H. Vincent Poor, (2003) *Wireless Communication Systems: Advanced Techniques for Signal Reception*. Prentice Hall. EUA
- Wave ACCESS NET (1999) en *Lucent Technologies Bell Labs Innovations*. [En línea]. Disponible en: comtech.supermicro.ca/comtech/productBrochures/DSLUCENW102400.PDF [Accesado el día 14 de mayo de 2007]
- Zyrem, J. (2001). “IEEE 802.11g Explained” en *Forskningsnett.Uninett* [En línea]. [En línea]. Disponible en: http://forskningsnett.uninett.no/wlan/download/WP_IEEE802gExpla_12_06.pdf [Accesado el día 11 de abril de 2007]
- Zyren, J. (2002). “Supporting Backward Compatibility in 802.11g” en *CommsDesign and EE community*. [En línea]. Disponible en: <http://www.techweb.com/encyclopedia/defineterm.jhtml?term=CCK%2FOFDM> [Accesado el día 24 de abril de 2007]
- ZyXel (2005). G-3000h: 802.11g: Wireless Access Point: User’s Guide, v. 3.50

ANEXOS


Anexo I Puntos de Acceso

Producto	Descripción	Precio
	Buffalo [WHR-HP-G54-2] AirStation High Power Wireless Cable/DSL Smart Router Conector Antena RP-SMA Hembra	62,95EUR
	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 Atheros	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



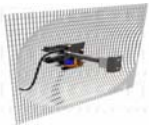
Anexo II Antenas Omnidireccionales

Productos	Descripción	Precios
	[AO24-15DBEXNH] de 15dBi para 2,4GHz Exterior Con Conector 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 Conector N Hembra	78,95EUR
	Ovislink [WAE-85] de 8,5dBi para 2,4GHz Exterior Con Conector 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


GLOSARIO

	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
	CyberBajt [CYB-PA-16DBI-NH] de 16dBi para 2,4GHz para Exterior Conector N Hembra	32,40EUR
	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 88° x 8° para 2,4Ghz Exterior Con Conector N Hembra	109,95EUR

GLOSARIO

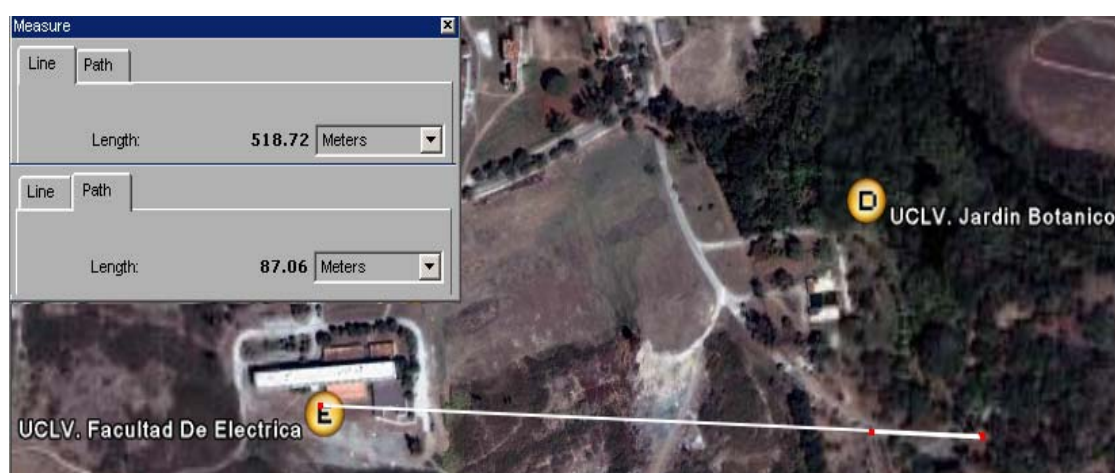
	Interline [INT-SEC-17-24-V] de 17dBi para 2,4Ghz Exterior Con Conector N Hembra	114,95EUR
---	--	-----------

Anexo VI Kit de Instalación

Producto	Descripción	Precio
	Kit 2 Senao Engenius AP NOC-3220-EXT Wireless Exterior Antena Parabolica SD19 + Pigtail 1,5M LMR-400 (400mW)	464,95EUR
	Kit Buffalo Router Punto de Acceso WHR-G54S Pigtail de 1,5 metros LMR-195 Antena Panel Interline 14dBi 2,4GHz	79,95EUR
	Kit Linksys Router AP WRT54GL-EU Antena Omnidireccional 15 dBi 2,4GHz + Pigtail 3 metros LMR- 400	129,90EUR

Fuente: Wimaxcom

Anexo VII Distancia entre los puntos de Jardín Botánico y la FIE.



Anexo VIII Canales de Frecuencia para los diferentes países

Canal	US / Canadá	Europa	Francia	España	Japón
1	2412	2412	-	-	2412
2	2417	2417	-	-	2417
3	2422	2422	-	-	2422
4	2427	2427	-	-	2427
5	2432	2432	-	-	2432
6	2437	2437	-	-	2437
7	2442	2442	-	-	2442
8	2447	2447	-	-	2447
9	2452	2452	-	-	2452
10	2457	2457	2457	2457	2457
11	2462	2462	2462	2462	2462
12	-	2467	2467	-	2467
13	-	2472	2472	-	2472
14	-	-	-	-	2484

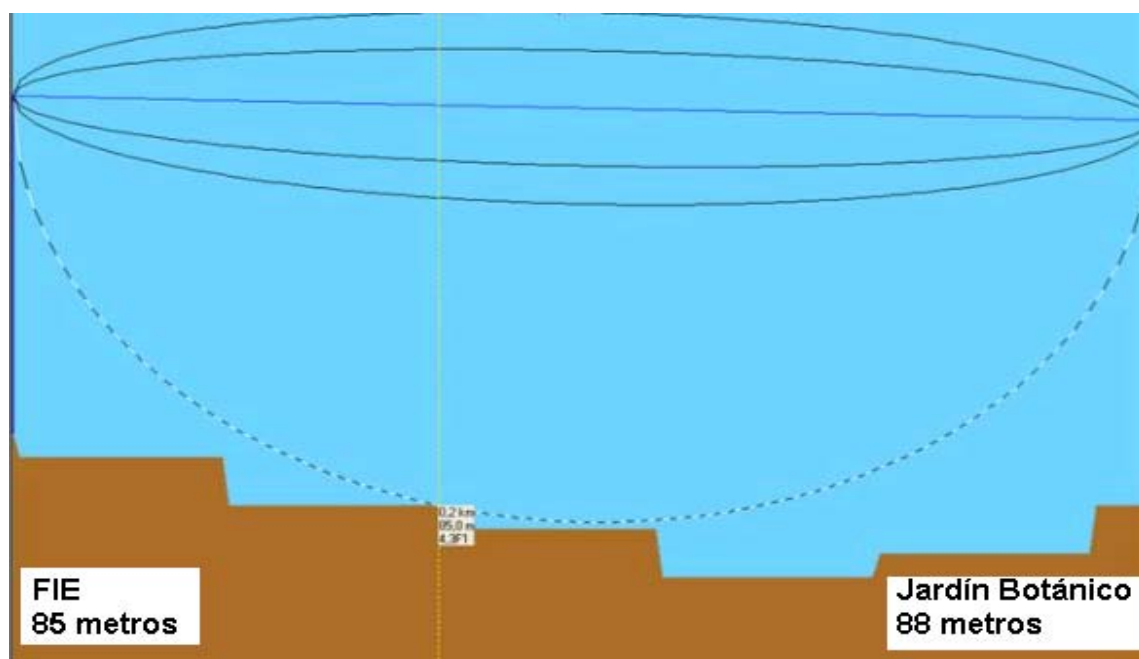
Anexo IX Hoja de cálculo utilizada para estimar la distancia de alcance máxima.

Cálculo de distancia alcance entre antenas

f (Frecuencia) = MHz En España Canal 11
 Z (Impedancia sistema) = omnis
 P_{TX} (Potencia entregada a antena transmisora) = dBm (NaN dBW, NaN mW, NaN W)
 S_{RX} (Sensibilidad en receptor) = dBm (NaN dBW, NaN mW, NaN W)
 M (Márgen ganancia para permitir error datos digital aceptable) = dB
 G_{TX} (Ganancia antena transmisora respecto isotrópica) = dBi
 Cable de metros con atenuación de dB/m = 0 dB
 G_{RX} (Ganancia antena receptora respecto isotrópica) = dBi
 Cable de metros con atenuación de dB/m = 0 dB

P_{rad} (Potencia radiada en antena transmisora) = NaN dBW (NaN dBm, NaN W, NaN mW)
 P_{req} (Potencia requerida en antena receptora) = NaN dBW (NaN dBm, NaN W, NaN mW)
 D (Distancia máxima entre antenas) = NaN Km

Anexo X Estimación de la zona de Fresnel según el Software Profesional Cobra



Anexo XI Equipos K-BEST para determinadas aplicaciones



Anexo XII Listado de equipos de la marca K-BEST que oferta Copextel en Cuba.

Descripción	U	Precio
BL3000 SERIES		
BL3005 Kbest P - MP 2.4GHz with integrated 18 dBi Flat Panel Antenna 802.11 (DSSS) 0.1 W	Uno	1,699.75
BL3006 Kbest P - MP 2.4GHz with integrated 18 dBi Flat Panel Antenna 802.11 (DSSS) 0.5 W	Uno	1,47.63

GLOSARIO

BL3007 Kbest P - MP 2.4GHz with integrated 18 dBi Flat Panel Antenna 802.11 (DSSS) 1 W	Uno	2,080.42
BL3008 Kbest P - MP 2.4GHz with integrated 18 dBi Flat Panel Antenna 802.11 (DSSS) 2 W	Uno	2,390.27
BL3201 Kbest P - MP 2.4GHz with integrated 18 dBi Flat Panel Antenna 802.11g (OFDM) 0.1 W	Uno	1,416.45
BL3202 Kbest P - MP 2.4GHz with integrated 18 dBi Flat Panel Antenna 802.11g (OFDM) 0.5 W	Uno	1,903.36
BL3203 Kbest P - MP 2.4GHz with integrated 18 dBi Flat Panel Antenna 802.11g (OFDM) 1 W	Uno	2,124.68
BL3016 Kbest P - MP 5.8 GHz with integrated 24 dBi Flat Panel Antenna 802.11 (DSSS) 0.2 W	Uno	2,213.21
BL3411 Kbest P - MP 5.8 GHz with integrated 24 dBi Flat Panel Antenna 802.11a (OFDM) 18dBm	Uno	1,991.89
BL3412 Kbest P - MP 5.8 GHz with integrated 24 dBi Flat Panel Antenna 802.11a (OFDM) 0.5 W	Uno	2,655.85
BL34B1 Kbest P - MP 5.8 GHz with integrated 22 dBi Flat Panel Antenna 802.11a (OFDM) 18dBm	Uno	1,991.89
BL34B2 Kbest P - MP 5.8 GHz with integrated 22 dBi Flat Panel Antenna 802.11a (OFDM) 0.5 W	Uno	2,655.85
BL 4000 SERIES		
BL4001 Kbest P - MP 2.4 GHz (Need to use external Antenna) 802.11b (DSSS) 0.1 W	Uno	1,239.40
BL4002 Kbest P - MP 2.4 GHz (Need to use external Antenna) 802.11b (DSSS) 0.5 W	Uno	1,593.51
BL4003 Kbest P - MP 2.4 GHz (Need to use external Antenna) 802.11b (DSSS) 1 W	Uno	1,726.30
BL4004 Kbest P - MP 2.4 GHz (Need to use external Antenna) 802.11b (DSSS) 2 W	Uno	2,036.15
BL4201 Kbest P - MP 2.4 GHz (Need to use external Antenna) 802.11g (OFDM) 0.1 W	Uno	1,106.61
BL4202 Kbest P - MP 2.4 GHz (Need to use external Antenna) 802.11g (OFDM) 0.5 W	Uno	1,637.78
BL4203 Kbest P - MP 2.4 GHz (Need to use external Antenna) 802.11g (OFDM) 1 W	Uno	1,859.10
BL4012 Kbest P - MP 5.725-5.85 GHz (Need to use external Antenna) 802.11b (DSSS) 0.3 W	Uno	2,213.21
BL4411 Kbest P - MP 5.725-5.85 GHz (Need to use external Antenna) 802.11a (OFDM) 18 dBm	Uno	1,637.78
BL4412 Kbest P - MP 5.725-5.85 GHz (Need to use external Antenna) 802.11a (OFDM) 0.5 W	Uno	2,301.74
BL44B1 Kbest P - MP 5.4-5.7 GHz (Need to use external Antenna) 802.11a (OFDM) 18 dBm	Uno	1,637.78
BL44B2 Kbest P - MP 5.4-5.7 GHz (Need to use external Antenna) 802.11a (OFDM) 0.5 W	Uno	2,301.74
Descripción	U	Precio
ANTENAS		
Antena sectorial de 90° en 2.4 GHz Ganancia 16 dBi	Uno	433.96
Antena sectorial de 120° en 2.4 GHz Ganancia 12 dBi	Uno	607.55
KIT DE CABLES		
CBL-50	Uno	78.12
CBL-70	Uno	156.23

GLOSARIO

CBL-90		Uno	190.94
	Lighting Protector		
Protector Polyphaser IX-2H2DC48/W		Uno	98.06

Fuente: Copextel SA

Anexo XIII Posibles valores del factor de corrección de errores (FEC) para el equipo KBest

Modulacion	FEC		
	1/2	2/3	3/4
BPSK	6 mbps	—	9 mbps
QPSK	12 mbps	—	18mbps
16QAM	24	48 mbps	36mbps
64QAM	—	48 mbps	54 mbps

Fuente: K-Best technology

Anexo XIV Cobertura para cada tipo de modulación.

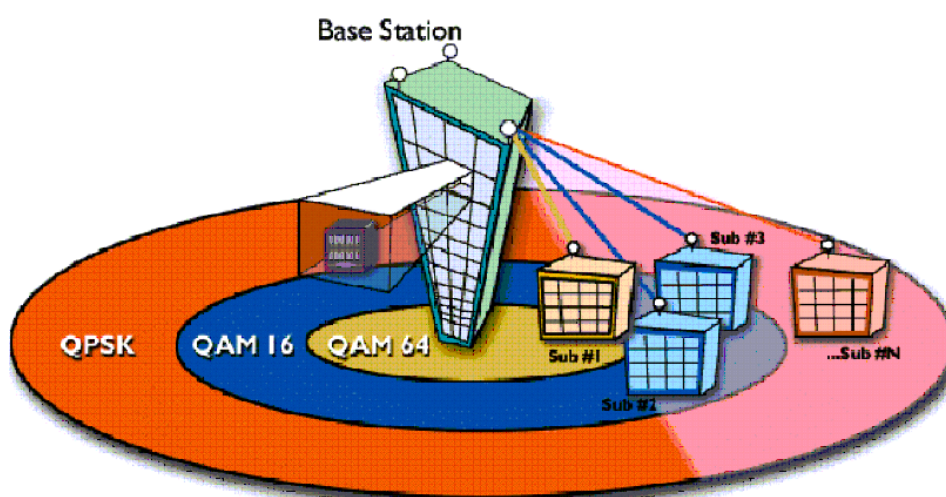
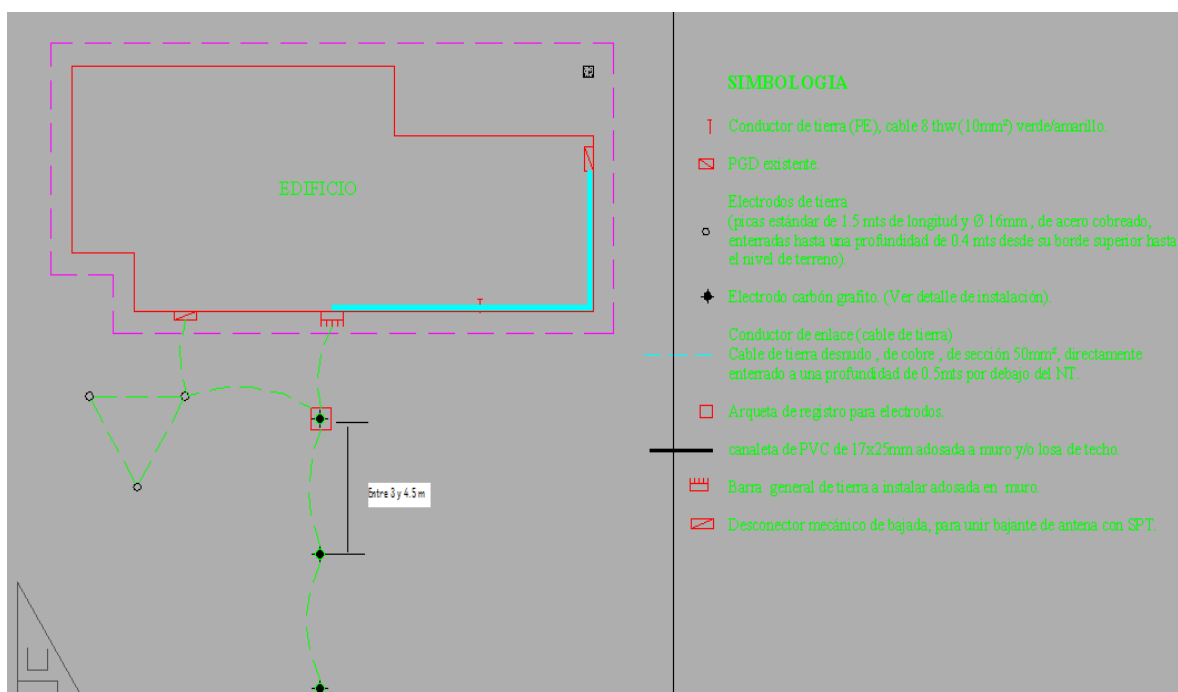
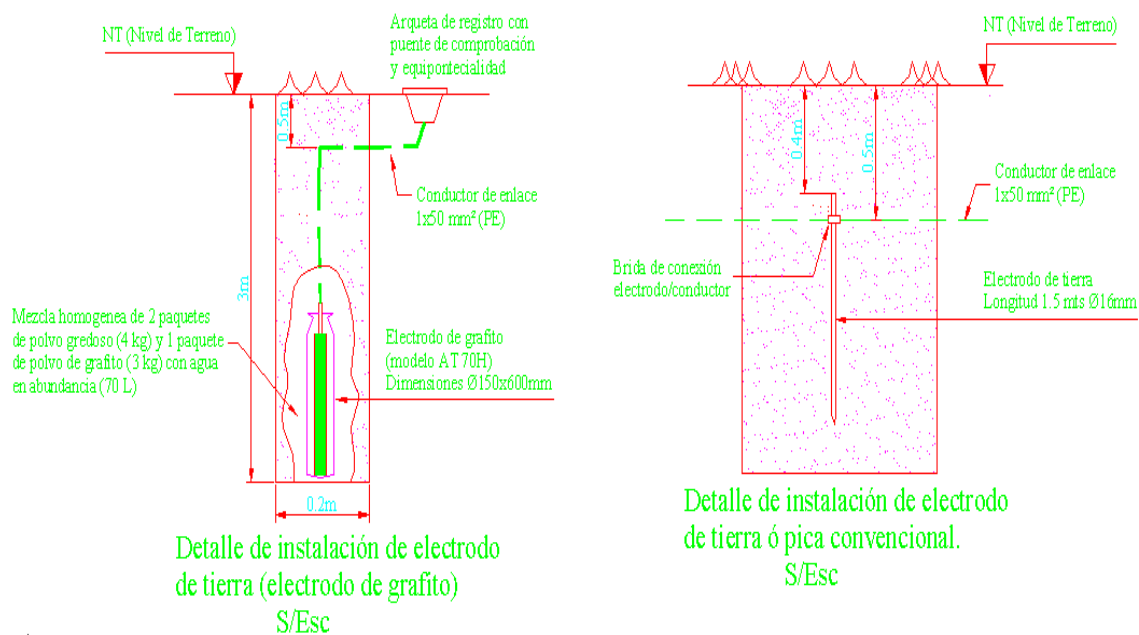


Figure 5: Adaptive Modulation and Coding

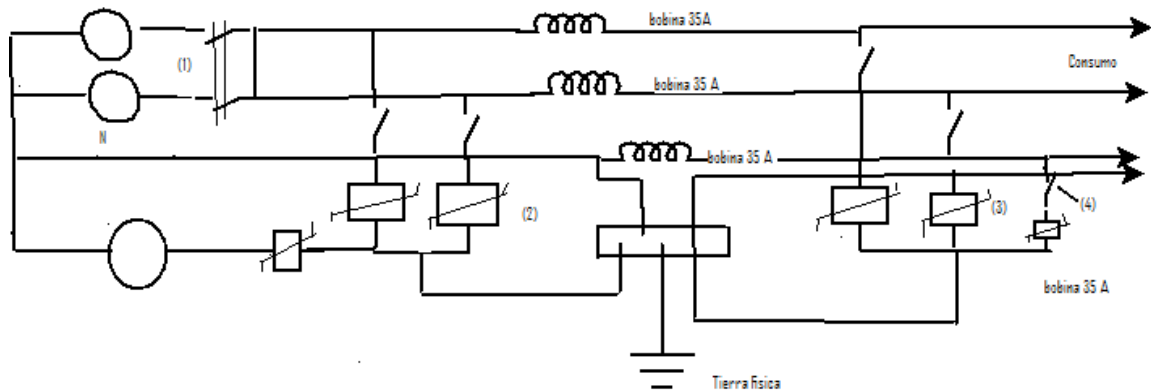
Anexo XV Diseño del sistema de tierra.



Anexo XVI Detalles de instalación de los electrodos de tierra. (Electrodo de grafito y de tierra o pica)



Anexo XVII Circuito Eléctrico de la Pizarra de distribución (PGD) para la protección del sistema de tierra.



Leyenda:

- (1) Desconectivo principal
- (2) Supresor DS 150E=120v (3 unidades)
- (3) Inductancia de acoplamiento (3 unidades)
- (4) Supresor AT 8215 (3 unidades)

Anexo XVIII Factor climático que interviene en la velocidad de transferencia de los datos en los enlaces inalámbricos.

Climate/Terrain Factor	
Value	Description
Good (C=0.25)	Mountains and dry climate
Average (C=1)	Average terrain and climate
Moderate (C=2)	Moderate terrain and climate
Difficult (C=4)	Over water or humid climate
Very Difficult (C=6)	Exterme humid climate
Close	

GLOSARIO

ANSI (American National Standards Institute) Instituto Nacional de Normas Americano.

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

BPSK (*Binary Phase Shift Keying*) Modulación por Desplazamiento de la Fase de dos Estados.

BRAN (*Broadband Radio Access Networks*) Redes de Acceso de Radio de Banda Ancha.

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.

DBPSK (*Differential Binary Phase Shift Keying*) Modulación Digital de Fase Diferencial Binaria.

DCF (*Distributed Coordinate Function*) Función de Coordinación Distribuida.

DFS (*Dynamic Frequency Selection*) Selección Dinámica de Frecuencia.

DLC (*Data Link Control*), Control del Enlace de Datos.

DLL (*Data Link Layer*) Nivel de enlace de datos.

DNS (*Domain Name Server*) Servidor de nombres de Dominio)

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

DTIM (*Delivery Traffic Indication Message*). Mensaje de indicación del tráfico enviado.

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

EAP-LEAP (*Light Extensible Authentication Protocol*) Protocolo de Autenticación Extensible Ligero.

EAP-PEAP (*Protected Extensible Authentication Protocol*) Protocolo de Autenticación Extensible Protegido.

EIA (Electronic Industries Alliance) Alianza de las industrias electrónicas

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

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

EMI (Interfase electromagnética).

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

FCC (*Federal Communications Commission*) Comisión Federal de Comunicaciones,
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.

IAPP (*Inter-Access Point Protocol*) Protocolo entre Puntos de Acceso.

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

IBSS (*Independent 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 la redes LAN inalámbricas.

IP (Internet Protocol) Protocolo de Internet.

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

ISO (*International Standard Organization*) Organización Internacional de Estándares.

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.

PGD (Pizarra General de distribución)

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

PIRE (*Potencia Isotrópica Radiada Equivalente*) Resultado del producto de la potencia suministrada a la antena por la ganancia isotrópica de esta.

RTS (Request to send) Solicitud de envío.

PSK (*Pre Shared Key*) Llave PreCompartida.

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

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

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

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

SEN (Sistema Electroenergético Nacional)

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).

SS (*Spread Spectrum*) Espectro Extendido.

TCP (*Transport Control Protocol*) 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 (*Transmitter Power Control*) Control de Potencia del Transmisor.

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

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

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

VHF (Very High Frequency) 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 Metropolitan 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.