



UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIA Y TECNOLOGIA

**Modelo de Red Wi-Fi para Campus Universitario
Caso: Universidad del Azuay**

*Tesis previa a la obtención del
Título de Mst. en Telemática*

AUTORES: Ing. Milton José Pérez Chango
Ing. Pablo Esteban Esquivel León

DIRECTORES: Ing. Fernando Balarezo

**Cuenca - Ecuador
2007**

**Todo el estudio, ideas y conceptos contenidos en esta tesis
son de exclusiva responsabilidad de los autores:**

Ing. Pablo Esquivel León

Ing. Milton José Pérez Chango

Dedicatoria:

**A mi esposa Yadira, por ser esa
mujer con que todo hombre
sueña.**

Pablo

Dedicatoria:

**A mi esposa Ximena, mi
Hija Camila y a mis padres, por
su tiempo sacrificado, su amor y
su apoyo incondicional brindado
para el desarrollo de esta tesis.**

Miltón

Agradecimiento:

A la Universidad del Azuay, y por su intermedio a las personas que la conforman y de manera particular al Ing. Fernando Balarezo por su valiosa guía durante el desarrollo de la tesis.

Resumen

El presente trabajo tiene como objeto crear un plan a seguir para la implementación de un Red Wireless en la Universidad del Azuay, utilizando para esto cálculos y modelos de propagación, software libre y herramientas de simulación de propagación.

El modelo utilizado para el cálculo de propagación es el ‘Log-normal Shadowing Path Loss Model’ ya que es un modelo que utiliza datos reales adquiridos en el en el lugar donde se realiza el estudio de propagación. Para la parte de seguridad y autenticación se verá la implementación de un portal cautivo en este caso se utilizará el software Nocat y además se realizará la configuración de VLans para de esta forma crear una red LAN virtual con el objeto de aislar la red Wireless de la red Lan con que cuenta la Universidad del Azuay

Abstract

The present work must like object create a plan to follow for the implementation of a Network Wireless in the University of the Azuay, using for this calculations and models of propagation, free software and tools of propagation simulation. The model used for the calculation of propagation is the “Log-normal Shadowing Path Loss Model” since it is a model that uses collected real data in in the place where the propagation study is made. For the part of security and authentication the implementation of a captive vestibule in this case will be seen will be used software Nocat and in addition the configuration of VLans will be made stops of this form to create a virtual network LAN with the intention of isolating the network Wireless of network LAN whereupon it counts the University of the Azuay

ÍNDICE

CAPITULO I REDES INALÁMBRICAS

1.1	Introducción	1
1.2	Elementos básicos de una red inalámbrica	1
1.3	Estándares WiFi de conexión	2
1.4	Clasificación de las redes inalámbricas	5
1.4.1	WAN/MAN (Wide Area Network/Metropolitan Area Network)	5
1.4.2	LAN (Local Area Network)	6
1.4.3	PAN (Personal Area Network)	6
1.5	Redes locales inalámbricas (Wlan)	6
1.6	Topología de las Wlan	8
1.6.1	Configuración Peer-to-Peer (Ad-Hoc)	8
1.6.2	Configuración en modo Punto de Acceso	8
1.7	Capas del IEEE 802.11	9
1.7.1	IEEE 802.11: Capa Física	9
1.7.1.1	Espectro Ensanchado por Salto de Frecuencia (FHSS)	9
1.7.1.2	Espectro Ensanchado por Secuencia Directa (DSSS)	10
1.7.1.3	Infrarrojo	12
1.7.2	IEEE 802.11: Capa de Enlace (MAC)	12
1.8	Operativa básica en una Wlan	12
1.8.1	Conexión a una celda	13
1.8.2	Proceso de autenticación y asociación	13
1.8.3	Itinerancia o Roaming	13
1.9	Factores en la propagación inalámbrica	15
1.9.1	Antenas	15
1.9.2	Puntos de Acceso Inalámbricos / Access Points	16
1.9.3	Interferencias y ruido	17
1.10	Cobertura Wlan Indoor	19
1.10.1	Límites de Emisión en WLAN	19
1.10.2	Umbral mínimo de recepción	20
1.10.3	Propagación de ondas radioeléctricas indoor	20
1.10.3.1	Propagación en espacio libre (LOS)	20
1.10.3.2	Propagación en Línea con Obstáculos (NLOS)	20

CAPITULO II REQUERIMIENTOS PARA IMPLEMENTAR UN MODELO DE COBERTURA Y PROPAGACIÓN EN Wlan

2.1	Objetivo y tipo de modelo	22
2.2	Uso de la Radiosidad	22
2.3	Modelos de propagación indoor	23
2.4	Modelos empíricos de propagación de ondas electromagnéticas.....	24
2.4.1	Modelo de propagación en el espacio libre	24
2.4.2	Log-normal shadowing path loss model	26
2.4.3	Modelo de pérdida de trayecto basado en cost 231	27
2.4.4	Modelo basado en el número de muros y suelos (simplificado)	28
2.4.5	Modelo UIT-R(unión internacional de telecomunicaciones)	29
2.4.6	Modelo de Atenuación lineal de la trayectoria	29
2.5	Modelos teóricos de propagación de ondas electromagnéticas.....	29

2.5.1	Modelos basados en ray-tracing	29
2.5.2	Modelos FDTD (finite-difference time-domain)	30
2.6	Propagación en línea con obstáculos (nlos)	31
2.6.1	Reflexión	31
2.6.1.1	Desvanecimiento por multitrayecto debido a reflexiones	32
2.6.1.2	Perfil de retardo	32
2.6.2	Penetración	33
2.6.3	Difracción	34
2.6.4	Dispersión	34

CAPITULO III

ANÁLISIS DE LA RED ACTUAL Y DISEÑO DEL MODELO

3.1	Antecedentes	36
3.2	Estructura de la Red Actual	36
3.2.1	Edificio de la Facultad de Administración	38
3.2.1.1	Procedimiento y Aplicación para los Cálculos	42
3.2.2	Edificio de Administración Central	45
3.2.3	Edificio de la Facultad de Filosofía	47
3.2.4	Edificio de la Facultad de Diseño	47
3.2.5	Laboratorio de Electrónica	50
3.3	Cálculos del Modelo	52
3.4	Conclusiones	55

CAPITULO IV

HERRAMIENTAS DE SIMULACIÓN DE PROPAGACIÓN

4.1	Evaluación de Herramientas	57
4.2	Radiowave Propagation Simulator (RPS)	57
4.2.1	Descripción del Uso del Programa de Simulación	58
4.3	Simulación del Edificio de Administración Planta Baja	62
4.4	Simulación de Administración piso 1	63
4.5	Simulación de Administración piso 2	64
4.6	Simulación de Administración piso 3	65
4.7	Simulación de Administración piso 4	66
4.8	Simulación de Filosofía planta baja	67
4.9	Simulación de Filosofía piso 1	68
4.10	Simulación de Filosofía piso 2	69
4.11	Simulación de Filosofía piso 3	70
4.12	Simulación de Filosofía piso 4	71
4.13	Simulación de Laboratorio de electrónica	72
4.14	Simulación del decanato de investigaciones y centro de cómputo planta baja	73
4.15	Simulación de la facultad de ciencias y tecnología.	74
4.16	Simulación del edificio de administración central	75
4.17	Simulación de la facultad de diseño	76
4.18	Simulación de la biblioteca	77
4.19	Propuesta de ubicación y mejoramiento de áreas de cobertura en cada sector de La Universidad del Azuay.	78
4.19.1	Administración planta baja	78
4.19.2	Administración piso 1	78
4.19.3	Administración piso 2	79
4.19.4	Administración piso 3	80
4.19.5	Administración piso 4	81

4.19.6	Filosofía planta baja	82
4.19.7	Filosofía piso 1	83
4.19.8	Filosofía piso 2	84
4.19.9	Filosofía piso 3	85
4.19.10	Filosofía piso 4	86
4.19.11	Laboratorio de electrónica	87
4.19.12	Decanato de investigaciones y centro de cómputo planta baja.....	88
4.19.13	Facultad de ciencias y tecnología.	91
4.19.14	Edificio de administración central	95
4.19.15	Facultad de diseño	96
4.19.16	Biblioteca	98

CAPITULO V

SEGURIDAD EN REDES WLAN

5.1	Mecanismos de Seguridad	99
5.2	Mecanismo de Seguridad Escogido para la Red de La Universidad del Azuay...	102
5.3	Nocat Auth	102
5.4	Instalación y Configuración de Nocat Auth	103
5.4.1	Instalación del Software Nocat	104
5.4.2	Configuración del portal /usr/local/nocat/nocat.conf	105
5.4.3	Configuración del Gateway /usr/local/nocat/gateway/nocat.conf	107
5.4.4	Configuración del archivo /etc/httpd/conf.d/ssl.conf	109
5.4.5	Configuración de las Interfaces	109
5.4.6	Configuración del cliente	110
5.4.7	Creación de la base de datos de los usuarios	110
5.4.8	Creación de Usuarios para Nocat	110
5.4.9	Iniciando el servidor de Nocat Auth	110
6	Seguridad en la Red	114
6.1	Configuración de la Vlan	114

CONCLUSIONES	116
RECOMENDACIONES	117
BIBLIOGRAFÍA	118
GLOSARIO	119
ANEXO 1 Croquis y ubicación de los Access Point	121
ANEXO 2 Tablas de cálculos del modelo de propagación para cada Access Point	126

CAPITULO 1

REDES INALÁMBRICAS

1.1 INTRODUCCIÓN

El desarrollo tecnológico en los últimos años ha tenido un avance sin precedentes en la historia, en estos tiempos poseemos equipos muy sofisticados en nuestros hogares, computadores, palm's, equipos reproductores de audio y video, teléfonos convencionales, teléfonos celulares, etc.; y la modalidad para la conexión o comunicación entre estos equipos o entre un equipo y la red tiende a ser e forma inalámbrica. Por lo tanto se ve un aumento de las redes de área local inalámbricas conocidas como WLAN (Wireless Local Área Network) y han ganado mucha popularidad. Es de interés en este capítulo dar a conocer todos los conceptos sobre WLAN's pero cabe indicar que son solo una pequeña parte de las redes inalámbricas como se verá en una futura clasificación.

Una WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar; la red por sí misma es móvil, es decir elimina la necesidad de usar cables y establece nuevas aplicaciones con flexibilidad. Lo más importante, incrementa la productividad y eficiencia en bs lugares donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e incluso sobre áreas metropolitanas.

Las redes WLAN permiten entre otras cosas: la incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

1.2 ELEMENTOS BÁSICOS DE UNA RED INALÁMBRICA¹

Existen algunos elementos necesarios dentro de una red inalámbrica.

a) Punto de Acceso Inalámbrico (Wireles Access Point)²

En redes de computadoras, un punto de acceso inalámbrico es un dispositivo que conecta dispositivos de comunicación inalámbrica entre sí para formar una red inalámbrica. Un WAP generalmente se conecta a una red inalámbrica y puede retransmitir datos entre dispositivos inalámbricos y dispositivos alambrados. Aquellas redes en donde los dispositivos se administran a sí mismo (sin la necesidad de un punto de acceso) son llamadas redes ad-hoc. En el punto 1.9.2 se explica sus características.

b) Dispositivos Móviles

¹ Cisco Systems, Inc. Academia de Cisco System; Guía del primer año CCNA 1 y 2. Tercera Edición. Pag 86,87

² <http://www.alegsa.com.ar>

Los hay muy diversos como computadores portátiles (Notebooks), PDAs , teléfonos celulares. Estos tienen instalados tarjetas PCMCIA o dispositivos USB con capacidades WI-FI y pueden, por lo tanto, recibir o enviar información a los Puntos de Acceso o a otros dispositivos de manera inalámbrica (RF). En la actualidad ya abundan los que tienen la tecnología WI-FI incorporada en el procesador (Intel, Atheros, etc.) y por lo tanto no necesitan de agregados USB o PCMCIA.

c)Dispositivos Fijos

Los computadores de sobremesa o fijos (desktops), las impresoras, cámaras de vigilancia, etc. también pueden incorporar tecnología WI-FI y, por lo tanto, ser parte de una red inalámbrica.

d)Otros elementos

También existen amplificadores y antenas que se pueden agregar, según las necesidades, a instalaciones WI-FI y sirven para direccionar y mejorar las señales de RF transmitidas

1.3 ESTÁNDARES WIFI DE CONEXIÓN

A partir del estándar IEEE 802.11/ WIFI se fueron desarrollando otros estándares relacionados con WIFI que han ido introduciendo mejoras y solucionando inconvenientes. En la figura 1.1 se observa los estándares en WIFI :

Estándares WIFI de Conexión

Estándar	Velocidad Máxima	Banda Frecuencia
802.11	1 y 2 Mbps	2.4 Ghz
802.11a	54 Mbps	5.15 Ghz
802.11b	11 Mbps	2.4 Ghz
802.11g	54 Mbps	2.4 Ghz
802.11n Para 2008 -	> 100 Mbps	2.4 Ghz...40 Ghz

Enero 2007
Aprobado Segundo
Borrador

1

Figura 1.1 Estándares WIFI

a) Estándar 802.11: Fue el primero y las velocidades de 1 y 2 Mbps eran muy pequeñas y no permitían implementar aplicaciones empresariales de envergadura, por lo tanto se crearon nuevos grupos de trabajo para crear otros estándares.

¹ <http://centros5.pntic.mec.es/desanton/wq/hunt02/hunt.html>

b) Estándar 802.11a: Permite realizar transmisiones con velocidades máximas de 54 Mbps y opera en una banda de frecuencia superior a los 5 GHz, por lo tanto no es compatible con el estándar 802.11b y el estándar 802.11g. A pesar de ser el "a" es, prácticamente, el más nuevo pues esa banda de frecuencia estaba asignada en muchos países a fuerzas públicas (bomberos, cruz roja, etc) y recién últimamente está siendo liberada. Es muy útil, como veremos en otros capítulos, en ciertos casos. Por ejemplo para separar el tráfico o para zonas con mucho ruido e interferencias. Además con el estándar 802.11a se pueden llegar a utilizar hasta 8 canales no superpuestos.

c) Estándar 802.11b: Las conexiones funcionan a una velocidad máxima de 11 Mbps y opera en una banda de 2,4 GHz. Es el más popular pues fue el primero en imponerse y existe un inventario muy grande de equipos y dispositivos que manejan esta tecnología. Además, al ser compatible con el estándar 802.11g permitió la incorporación de éste último a las redes inalámbricas wifi ya existentes. Con el estándar 802.11b, sólo se pueden utilizar 3 canales no superpuestos (de los 11 existentes) en la mayoría de los países. En Europa, según los estándares ETSI, se pueden utilizar 4 canales de los 13 existentes. No todos los Puntos de Acceso Inalámbrico sirven para los 2 sistemas, así que es importante tenerlo en cuenta a la hora de adquirir un Access Point.

d) Estándar 802.11g: Las conexiones funcionan a una velocidad máxima de 54 Mbps y opera en una banda de 2,4 GHz. El estándar 802.11g fue aprobado a mediados del año 2003 y se popularizó rápidamente por su compatibilidad con el estándar 802.11b. Lo que muchos desconocen es que al mezclar equipos del estándar 802.11b con equipos del estándar 802.11g la velocidad la fija el equipo más lento, o sea que la instalación mixta seguirá funcionando generalmente a velocidades lentas. Respecto de los canales aquí caben las mismas observaciones que para el estándar 802.11b, o sea que con el estándar 802.11g se pueden utilizar 3 canales no superpuestos de los 11 disponibles y en Europa 4 de los 13 canales disponibles. Los canales que generalmente se utilizan con el estándar 802.11g y con el estándar 802.11b son: "1", "6" y "11" y en Europa: "1", "4", "9" y "13".

e) Estándar 802.11n: Es un estándar nuevo que aún está en elaboración. Si bien se está trabajando en él desde el año 2004, sólo se ha logrado hasta ahora un borrador, que todavía no es definitivo y que, como suele suceder, puede ser modificado hasta la aprobación final del estándar 802.11n. El objetivo es elaborar un estándar con velocidades de transmisión superiores a 100 Mbps. El proceso se está demorando pues entre los promotores del estándar se han formado dos grupos antagónicos WWiSE y TGn Sync. Ninguno de los dos tiene una mayoría suficiente para imponer su tecnología y por lo tanto están trabadas las negociaciones. En 2005 se creó otro grupo con empresas de ambos bandos para tratar de encontrar algún punto medio. Este grupo es el "Enhanced Wireless Consortium - EWC". En lo único que están los dos grupos de acuerdo es en la utilización de una nueva tecnología conocida como MIMO () que permite incrementar el ancho de banda y el alcance en WIFI utilizando Multiplexing. Según se apruebe la propuesta de un grupo u otro, las velocidades podrían variar entre 135 Mbps y 300 Mbps y las bandas de frecuencia serían 10GHz, 20GHz o 40GHz.

f) El Dilema Pre-estándar 802.11n: En las redes inalámbricas WIFI, el tema de la homologación y certificación de equipos, no es un tema menor. Conviene aclarar, desde ya, y enfatizar que la compra de equipos homologados y certificados por la WiFi Alliance (Organización que agrupa a los fabricantes de productos WiFi) es de vital

importancia para garantizar un funcionamiento armónico de los diversos elementos que componen una red inalámbrica wifi.

Por todo esto es importante dejar claro a todos los usuarios que cualquier producto que compren de 802.11n no es estándar y puede presentar ahora y, aún más en el futuro, problemas de compatibilidad con otros elementos de la red inalámbrica wifi.

Por otra parte, se dice que el futuro de wireless es WiMAX (Worldwide Interoperability for Microwave Access). ,promete ampliar la banda ancha inalámbrica reduciendo costos. Contrariamente al acceso inalámbrico Wi-Fi, que sólo permite la conexión con la Web dentro de zonas muy restringidas, las estaciones base de Wi-MAX podrían extender el espectro de conectividad a 50 kilómetros, lo que supone un gran avance en comparación con los 91 metros de Wi-Fi, y ni qué decir sobre los 9 metros de Bluetooth. La mayor distancia de cobertura es clave para permitir que los proveedores de servicios sean capaces de ofrecer acceso a Internet de banda ancha directamente a los hogares, sin tener que tender un cable físico hasta el final; lo que se conoce como la "última milla", que conecta a cada uno de los hogares o abonados con la red principal de cada proveedor. En la figura 1.2 se puede observar un resumen de la evolución de las redes inalámbricas.

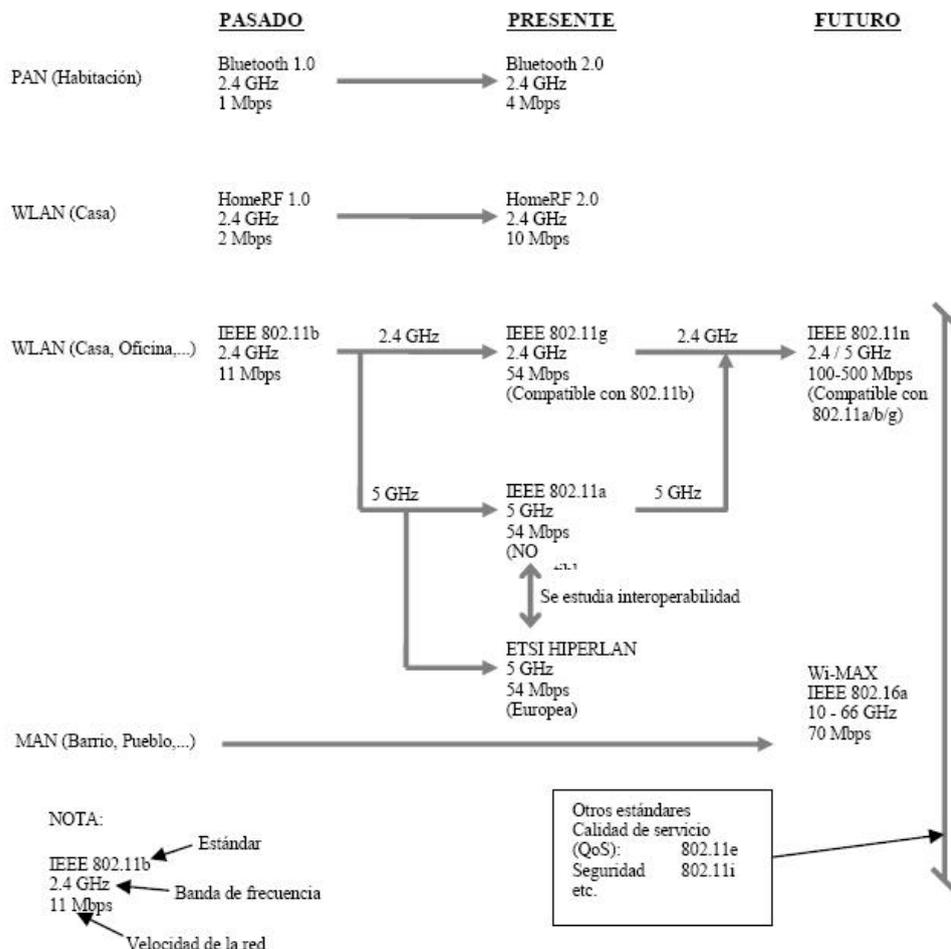


Figura 1.2 Evolución de las Redes Inalámbricas

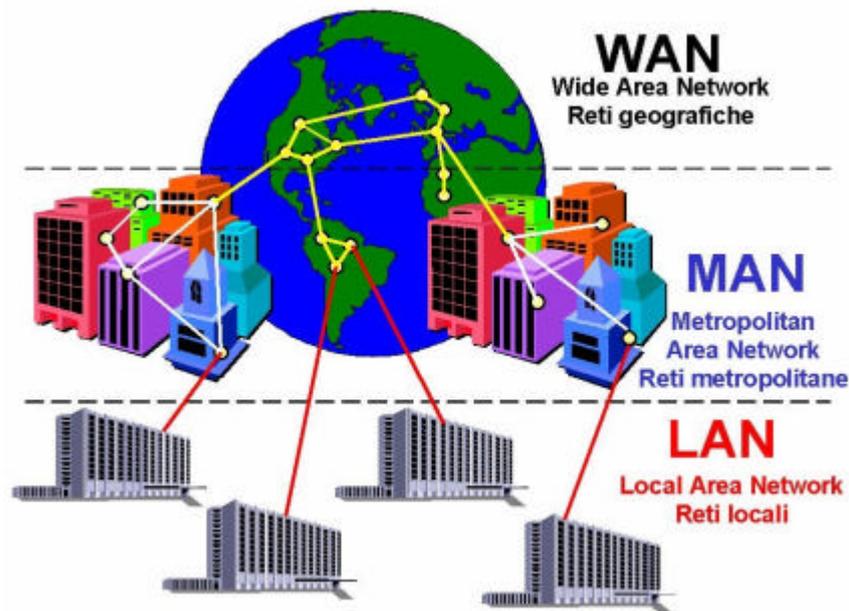
¹ <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

1.4 CLASIFICACION DE LAS REDES INALÁMBRICAS

Las redes inalámbricas, al igual que las redes tradicionales cableadas se clasifican en tres categorías.

- WAN/MAN (Wide Area Network/Metropolitan Area Network)
- LAN (Local Area Network)
- PAN (Personal Área Network)

En la figura 1.3 se muestran las características de las redes inalámbricas:



1

Figura 1.3 Características de las redes inalámbricas

1.4.1 WAN/MAN (Wide Area Network/Metropolitan Area Network)²

Estas redes cubren desde decenas hasta miles de kilómetros, cuya finalidad es la constitución de redes globales de comunicación móvil. Como ejemplo de estas redes se encuentran los siguientes sistemas:

- GSM (Global System for Mobile Communications): Sistema global de comunicaciones móviles de segunda generación (2G) que permite comunicaciones de hasta 9,6 Kbps.
- GPRS (General Packet Radio Service): Estándar de comunicaciones móviles que permite velocidades de hasta 115 Kbps.

¹ <http://www.sanluis.gov.ar/res/5762/img/redes/3545.jpg>

² Cisco Systems, Inc. Academia de Cisco System; Guía del primer año CCNA 1 y 2. Tercera Edición. Pág. 44,45

- UMTS (Universal Mobile Telecommunications System): Tecnología de comunicaciones móviles de tercera generación (3G) que ofrece velocidades desde 144 Kbps hasta 2 Mbps.

1.4.2 LAN (Local Area Network)

Estas comprenden distancias desde varios metros hasta decenas de metros. Permiten la creación de redes locales sin cables, realizando la comunicación por ondas de radio. La tecnología más conocida es el estándar 802.11 (o WiFi) que opera dentro de los 2.4 GHz (5 GHz 802.11a) y provee un ancho de banda de hasta 54 Mbps.

1.4.3 PAN (Personal Area Network)

En la categoría PAN se encuentran las redes que comprenden desde muy poca distancia hasta 30 metros. Se trata de redes personales que tienen como principal fin eliminar los cables de comunicación con todos los dispositivos electrónicos (PC con periféricos o accesorios, teléfonos móviles, cámaras...). Su principal exponente es la tecnología Bluetooth, pero existen otras como 802.15 y HomeRF.

1.5 REDES LOCALES INALÁMBRICAS (WLAN)¹

Una red de área local inalámbrica o WLAN (Wireless LAN) utiliza la tecnología de Radio frecuencia (RF) que, en lugar de los tradicionales y molestos cables, utiliza el aire como medio de comunicación mediante la transmisión de ondas Electromagnéticas.

Las redes locales inalámbricas más que una sustitución de las LANs convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario, minimizando la necesidad de establecer una conexión física cableada y ofreciendo al usuario conexión de datos de banda ancha y movilidad. En este sentido, el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas, enlazando los diferentes equipos o terminales móviles asociados a la red. Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aun así sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2, 11 ó 54 Mbps frente a los 10, 100 ó los 1000 Mbps ofrecidos por una red convencional actual.

Las aplicaciones de las redes de área local inalámbricas que podemos encontrar actualmente son muy variadas:

¹ Cisco Systems, Inc. Academia de Cisco System; Guía del primer año CCNA 1 y 2. Tercera Edición. Pág. 44,45

- Entornos difíciles de cablear. Implementación de redes de área local en edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Entornos en los que se debe permitir el acceso a la información mientras el usuario se encuentra en movimiento y en tiempo real.
- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo (exposiciones, acontecimientos deportivos, zonas catastróficas,...).
- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- Interconexión de redes de área local que se encuentran en lugares físicos distintos.
- Actualmente se están desplegando las denominadas Zonas IP, que son lugares públicos donde las WLAN ofrecen conexión a Internet: aeropuertos, estaciones de autobús, auditorios de congresos, hoteles y otros lugares públicos.

A continuación se enumeran las ventajas de las redes WLAN sobre las LAN cableadas:

- Movilidad
- Superior ancho de banda
- Libre utilización de la frecuencia de 2.4 Ghz
- Reducción de costes
- Velocidad simétrica
- Complemento perfecto de redes tradicionales con cableado
- Cobertura en zonas sin infraestructuras de telecomunicaciones
- Funcionamiento sin errores
- Escalabilidad

Entre las dificultades e inconvenientes que presentan las redes WLAN se pueden destacar los siguientes.

- Alcance limitado
- Seguridad
- Ancho de banda compartido
- Posibles interferencias
- Posibles repercusiones sobre la salud
- Confusión debida a la multiplicidad de estándares
- Difícil uso simultáneo en múltiples países

- Confusión debida a la multiplicidad de estándares
- Difícil uso simultáneo en múltiples países.

1.6 TOPOLOGÍA DE LAS WLAN¹

Las configuraciones o topologías se pueden dividir en dos grandes grupos, las redes Peer to Peer y las que utilizan Puntos de Acceso.

1.6.1 Configuración Peer-to-Peer (Ad-Hoc)

También conocidas como redes ad-hoc, es la configuración más sencilla ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas. En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red. En la figura 1.4 se muestra un ejemplo de esta configuración.



Figura 1.4 Red en configuración Peer to Peer

1.6.2 Configuración en modo Punto de Acceso

Conocidas como configuraciones en modo Infraestructura, utilizan el concepto de celda, ya utilizado en otros sistemas de comunicación inalámbrica como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de 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.

La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados Puntos de Acceso, que funcionan

¹ Cisco Systems, Inc. Academia de Cisco System; Guia del primer año CCNA 1 y 2. Tercera Edicion.Pag. 88-95

como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso. Los Puntos de Acceso son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un radio de al menos treinta metros.

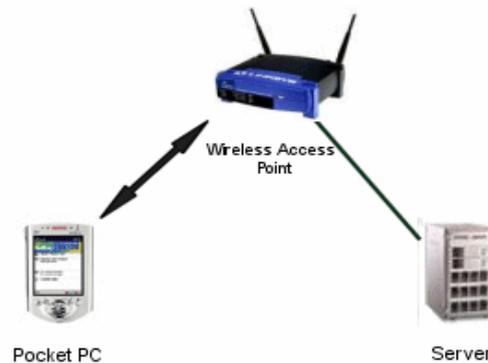


Figura 1.5 Red en configuración como punto de acceso

1.7 CAPAS DEL IEEE 802.11

Los estándares 802.x, cubren la capa física y la capa de enlace o MAC. El estándar 802.11 define tres capas físicas diferentes: espectro ensanchado por secuencia directa (DSSS), espectro ensanchado por salto en frecuencia (FHSS) e infrarrojos. La capa de enlace o MAC es común para las 3 capas físicas, proporcionando una interfase única a los protocolos de capas superiores.

1.7.1 IEEE 802.11: Capa Física¹

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. Los métodos de RF operan en la banda de frecuencia de 2.4 GHz, ocupando aproximadamente 83 MHz de ancho de banda entre los 2,400 y 2,483 GHz. El nivel potencia máximo permitido en este rango de frecuencias varía de un país a otro según sus normas regulatorias.

1.7.1.1 Espectro Ensanchado por Salto de Frecuencia (FHSS)²

La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo (llamado dwell time) inferior a 400 ms. Pasado este tiempo se

¹ <http://www.ieee.org/portal/site>

² www.senacitel.cl/downloads/senacitel2002/ID034.pdf

cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo. En la figura 1.6 se observa gráficamente los saltos de frecuencia.

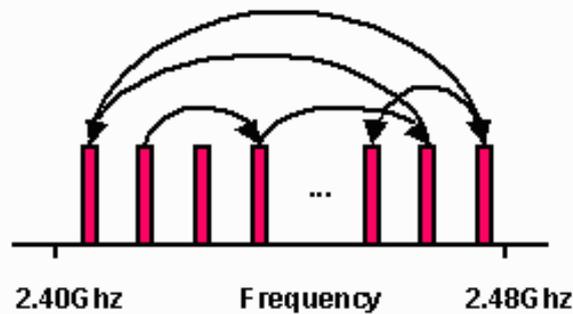


Figura 1.6 Codificación con saltos de frecuencia

El orden en los saltos en frecuencia se determina según una secuencia pseudo aleatoria almacenada en unas tablas, que tanto el emisor y el receptor deben conocer. El estándar IEEE 802.11 define la modulación aplicable, en este caso se utiliza la modulación en frecuencia FSK (Frequency Shift Keying), con una velocidad de 1 Mbps ampliable a 2 Mbps. En la revisión 802.11b del estándar, la velocidad también ha aumentado a 11Mbps. Una trama FHSS presenta un formato como el mostrado en la figura 1.7

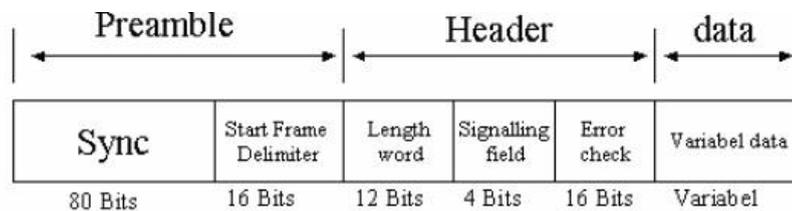


Figura 1.7 Formato de la trama FHSS²

El preámbulo y la cabecera son siempre transmitidos a 1 Mbps. El resto de la trama es transmitido a la velocidad indicada en el campo de señalización. Para minimizar el efecto de las reflexiones multitrayecto el FHSS tiene un salto de distancia mínima entre frecuencias. Esto es debido a que las reflexiones del salto anterior tienen un efecto mínimo sobre el siguiente salto debido a que, transcurrido el retardo producido por la reflexión hasta llegar al receptor, éste se encontrará entonces esperando por información en una frecuencia diferente.

1.7.1.2 Espectro Ensanchado por Secuencia Directa (DSSS)

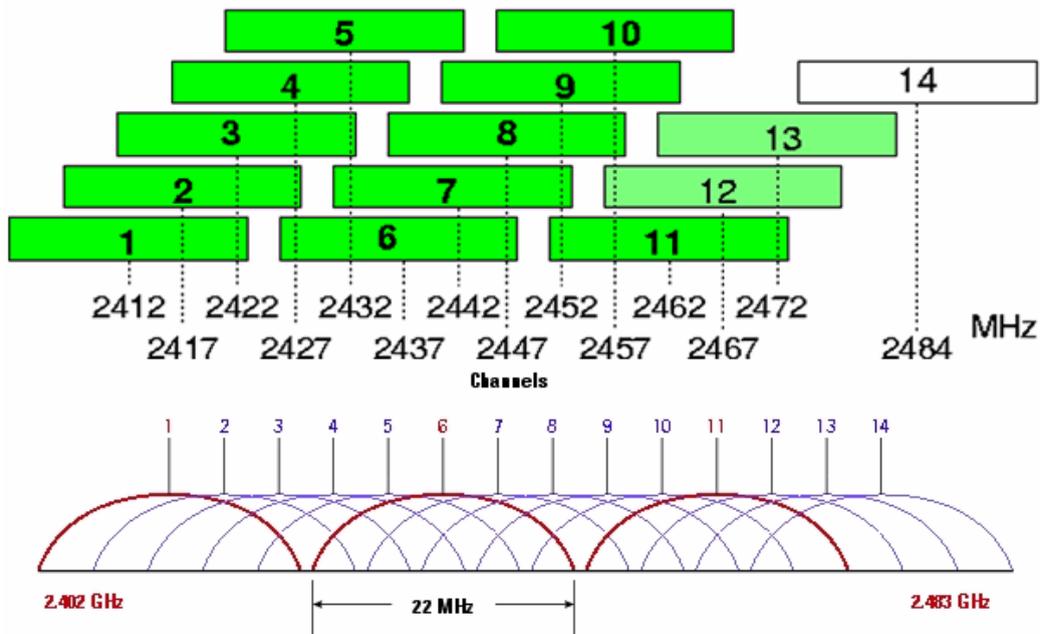
El espectro ensanchado por secuencia directa DSSS es el segundo nivel físico soportado por el 802.11 y el único especificado en el 802.11b, soportando velocidades de transmisión de 5.5 y 11Mbps. Con arreglo a 802.11 debe existir una separación de 30 MHz entre las frecuencias centrales de los canales si las celdas se solapan y/o son adyacentes para no causar interferencias. En 802.11b la separación se reduce a 25

¹ <http://www-personal.umich.edu/~csev/hng/book/08wireless/08wireless.htm>

² <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

MHz. Esto significa que pueden existir 3 celdas con zonas solapadas y/o adyacentes sin causar interferencias entre ellas, esto se observa en la figura 1.8.

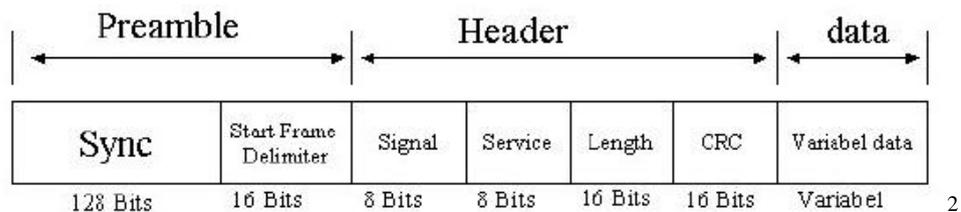
En configuraciones donde exista más de una celda, éstas pueden operar simultáneamente y sin interferencias, siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz.



1

Figura 1.8 Canales y valores de frecuencias DSSS

El estándar 802.11b utiliza DSSS en la banda de 2.40 GHz y la estructura de canales diseñada en el estándar 802.11. La principal diferencia entre los dos estándares gravita en que 802.11b utiliza modulación CCK (Complimentary Code Keying) para las velocidades de 5.5 Mbps y 11 Mbps. El 802.11b soporta también las velocidades de 1Mbps y 2 Mbps, por lo que tiene compatibilidad hacia atrás con los dispositivos 802.11. En la figura 1.9 se muestra el formato de trama DSSS.



2

Figura 1.9 Formato de trama DSSS

¹ www.air-stream.org.au/channel_802_11b

² <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

Al igual que en FHSS el preámbulo y la cabecera se transmiten siempre a 1 Mbps y el campo de señalización indica la velocidad de transmisión de los datos. En el 802.11b este campo soporta velocidades mayores que el original de 1 y 2 Mbps (5,5 Mbps y 11 Mbps).

1.7.1.3 Infrarrojo

El IEEE 802.11 no ha desarrollado todavía en profundidad esta área y solo menciona las características principales de la misma:

- Entornos muy localizados, un aula concreta, un laboratorio, un edificio.
- Modulaciones de 16-PPM y 4-PPM que permiten 1 y 2 Mbps de transmisión.
- Longitudes de onda de 850 a 950 nanómetros de rango.
- Frecuencias de emisión entre $3,15 \cdot 10^{14}$ Hz y $3,52 \cdot 10^{14}$ Hz.

Las WLAN por infrarrojos son aquellas que usan el rango infrarrojo del espectro electromagnético para transmitir información mediante ondas por el espacio libre. Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, similares a las que tiene la luz visible. De esta forma los infrarrojos son susceptibles de ser interrumpidos por cuerpos opacos pero se pueden reflejar en determinadas superficies.

1.7.2 IEEE 802.11: Capa de Enlace (MAC)¹

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas, ya que deben tenerse en cuenta las dos topologías de una red inalámbrica (modo independiente o infraestructura). Además se deben de tener en cuenta otros factores como son:

- Perturbaciones ambientales (interferencias).
- Variaciones en la potencia de la señal.
- Conexiones y desconexiones repentinas en la red.
- Roaming es decir nodos móviles que van pasando de celda en celda.

A pesar de todo ello la norma IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas, facilitando de este modo la fabricación en serie de chips. La principal función de esta capa es el control de acceso al medio, realizando igualmente funciones como fragmentación, encriptación, gestión de alimentación eléctrica, sincronización y soporte de roaming entre múltiples APs.

1.8 OPERATIVA BÁSICA EN UNA WLAN

Las 2 operativas más importantes que se producen en el funcionamiento de una WLAN son el método utilizado por una estación para conectarse a una celda y el soporte de roaming entre APs.

1.8.1 Conexión a una celda

¹ Cisco Systems, Inc. Academia de Cisco System; Guía del primer año CCNA 1 y 2. Tercera Edición. Pág. 239,249.

Existen 3 momentos en que una estación necesitará acceder a un BTS: después del encendido, al finalizar el sleep-mode o cuando entra en el área del BTS. La estación precisa obtener información de sincronización del Access Point (configuración en modo infraestructura) o de otra estación (configuración en modo independiente). La estación puede utilizar dos métodos para obtener esta información:

a) Active Scanning.- En este método la estación trata de localizar el Access Point transmitiendo tramas de petición de sondeo, quedando a la espera de paquetes de respuesta de sondeo desde el Access Point.

b) Passive Scanning.- En este método la estación se queda a la espera de recibir una trama Beacon del Access Point. La trama Beacon contiene la información de sincronización y proporciona a la estación la información que necesita.

El método utilizado por la estación dependerá de su consumo de energía y su propia operativa

1.8.2 Proceso de autenticación y asociación

Una vez que la estación ha localizado un Access Point y decide unirse a su BTS, debe iniciar un proceso de autenticación. Este proceso consiste en un intercambio de información entre el Access Point y la estación donde cada extremo prueba el conocimiento de una contraseña predefinida.

Realizado el proceso de autenticación, se inicia el proceso de asociación. La estación y el BTS intercambian información acerca de sus propias capacidades y el DSS toma conocimiento de la posición actual de la estación. Una estación no puede transmitir o recibir tramas de datos sin que el proceso de asociación haya concluido.

1.8.3 Itinerancia o Roaming

Los Puntos de Acceso Inalámbricos tienen un radio de cobertura aproximado de 100m, aunque esto varía bastante en la práctica entre un modelo y otro y según las condiciones ambientales y físicas del lugar (obstáculos, interferencias, etc)- ver: Pérdidas de Señal en Wifi. Si nos interesa permitir la itinerancia (roaming, en inglés) y movilidad de los usuarios, es necesario colocar los Access Point de tal manera que haya "overlapping" - superposición - entre los radios de cobertura, como indica la figura 1.10 vemos la zona de superposición indicada por la flecha roja y como es posible desplazarse de A a B, sin perder la señal de Wifi. El usuario está conectado al comienzo al Punto de Acceso A y en un determinado momento pasa a recibir la señal del Punto de Acceso B. Veremos como funciona este proceso.

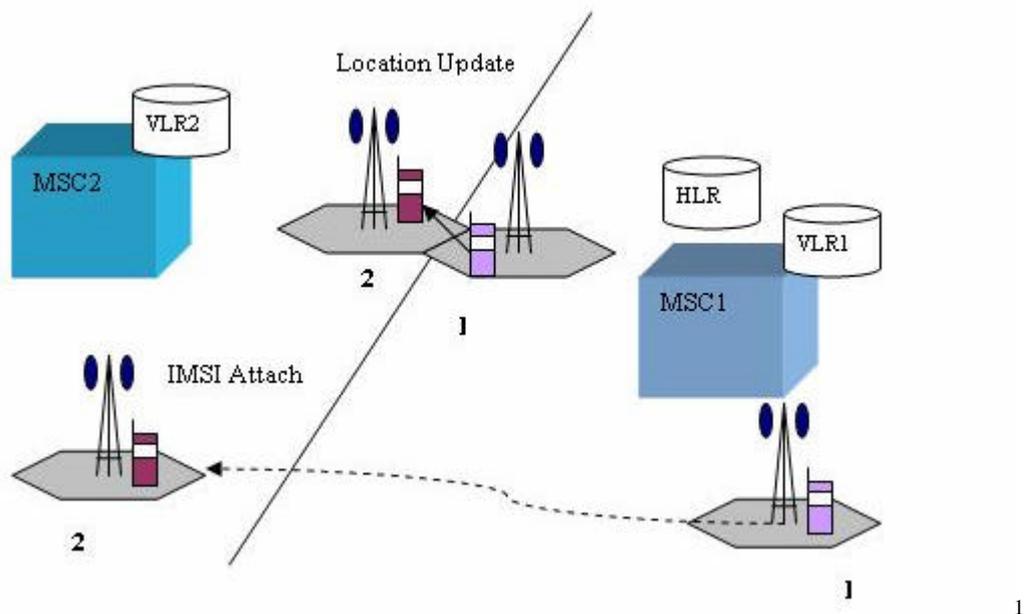


Figura 1.10 Roaming

a) El Roaming y los Paquetes Beacons.

- 1.- En la Transmisión de la Información en WiFi, los Puntos de Acceso Inalámbricos emiten intermitentemente unos paquetes denominados Beacons . Cuando una estación se aleja demasiado de un Access Point, "pierde la señal", es decir que deja de percibir estos Beacons que le indican la presencia del Access Point
- 2.- Si hay superposición, se comienzan a captar los Beacons del otro Access Point, hacia el cual se está dirigiendo, a la vez que se van perdiendo gradualmente los del anterior.

b) El Roaming y los Paquetes ACK

- 1.- También se vió en "Transmisión de la Información en Wifi" , que una vez que se envía un paquete de datos en las redes inalámbricas WiFi, la estación receptora envía un "O.K.", denominado ACK . Si la estación emisora se aleja demasiado de la transmisora, es decir que sale del radio de cobertura, no captará los ACK enviados.
- 2.- Los equipos de WIFI incorporan un algoritmo de decisión que debe determinar en que momento se desconectan del Access Point A y se conectan al Access Point B, como se ve en la figura.

c) La Problemática del Roaming

El estándar 802.11 WiFi, no contiene instrucciones detalladas sobre el tema del roaming, por lo tanto cada fabricante diseña el algoritmo de decisión según su criterio y con los parámetros que estima convenientes. Por esta razón pueden existir problemas, sobre todo en grandes ambientes, al mezclar Puntos de Acceso de diferentes fabricantes o Puntos de Acceso de un fabricante con dispositivos móviles de otras marcas. Cada uno tendrá otro algoritmo de decisión y pueden producirse "desavenencias" en el roaming.

¹ <http://upload.wikimedia.org/wikipedia/pl/6/69/Roaming.jpg>

1.9 FACTORES EN LA PROPAGACIÓN INALÁMBRICA

Existen un grupo de factores que afectan a la cobertura inalámbrica, algunos se producen en mayor medida que otros. En la figura 1.11 se muestran el grupo e factores que afectan la cobertura.

 <p>PUNTO DE ACCESO</p>		 <p>PC CARD</p>
<p>Tipo de Antena</p> <ul style="list-style-type: none"> ▪ Ganancia ▪ Patrón de radiación ▪ Efectos de la radiación ▪ Perdidas <p>Ubicación</p> <ul style="list-style-type: none"> ▪ Altura ▪ Ángulo ▪ Polarización <p>Otros aspectos:</p> <ul style="list-style-type: none"> ▪ Receptor RAKE ▪ Ecuilibradores ▪ Técnica de modulación ▪ Movimiento 	<p>Obstáculos</p> <ul style="list-style-type: none"> ▪ Penetración ▪ Reflexión ▪ Difracción ▪ Refracción ▪ Dispersión <p>Perdidas de propagación</p> <ul style="list-style-type: none"> ▪ Distancia ▪ Frecuencia <p>Interferencias</p> <p>Ruido</p>	<p>Tipo de Antena</p> <ul style="list-style-type: none"> ▪ Ganancia ▪ Patrón de radiación ▪ Efectos de la radiación ▪ Perdidas <p>Ubicación</p> <ul style="list-style-type: none"> ▪ Altura ▪ Ángulo ▪ Polarización <p>Otros aspectos:</p> <ul style="list-style-type: none"> ▪ Receptor RAKE ▪ Ecuilibradores ▪ Técnica de modulación ▪ Movimiento

Figura 1.11 Factores que afectan a la cobertura

1.9.1 Antenas

El tipo de antena influye en ambos extremos de la comunicación. Una antena es un dispositivo generalmente metálico capaz de radiar y recibir ondas de radio; que adapta la entrada/salida del receptor/transmisor al medio. La antena convierte las ondas eléctricas entregadas por el emisor, en ondas electromagnéticas que se pueden transmitir por el espacio libre; y en el otro extremo, convierte las ondas electromagnéticas que recibe, en ondas eléctricas que entrega al receptor. Básicamente su estructura consiste en un trozo de material conductor, al cual se le aplica una señal, y ésta es radiada por el espacio libre. Opera igualmente en sentido inverso, capturando la señal de radiofrecuencia del aire y entregándola posteriormente al receptor.

Las antenas juegan un papel vital en la definición del área de cobertura de una WLAN. Si se ignora su importancia los puntos de acceso podrían no conseguir los máximos radios de efectividad y cobertura, lo cual puede incurrir en un aumento de costes al ser

¹ <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

necesario un mayor número de puntos de acceso para cubrir el área requerida. Una elección correcta de antena incrementa los niveles de cobertura de su celda produciendo una reducción de costes, al ser necesarios un menor número de puntos de acceso. Las antenas presentan algunas características a ser consideradas:

- Ancho de banda
- Potencia
- Patrón de radiación
- Antena Isotrópica
- Ganancia de la antena
- Beam width (anchura de haz)
- Polarización de la Antena
- Resistencia de radiación

1.9.2 Puntos de Acceso Inalámbricos / Access Points

Existen diversos tipos de Puntos de Acceso Inalámbricos, se acostumbra a agrupar a los Access Point en dos categorías: Puntos de Acceso Básicos, "Thin" en inglés, y Puntos de Acceso Robustos, "Fat" en inglés.

Características de Puntos de Acceso Inalámbricos Básicos:

- Más económicos
- Más sencillos de gestionar y configurar
- Es más fácil compatibilizarlos con otras marcas

Características de Puntos de Acceso Inalámbricos Robustos:

- Son bastante inteligentes e incorporan funciones adicionales de gestión y seguridad
- Son más costosos
- Son más complicados de gestionar
- Sobrecargan el tráfico
- En algunos casos tienen slots libres para futuras actualizaciones

Algunas de las funciones de gestión y seguridad que incorporan los Puntos de Acceso Inalámbricos Robustos son:

Firewall

Utilidades para Site survey de redes inalámbricas

Opción de no emitir SSID

Antenas wifi opcionales

Ajuste de potencia

Las funciones extra que incorporan los Access Point Fat - Robustos, se terminan pagando. Por ello es importante evaluar seriamente, si está previsto utilizar esas funciones adicionales y si no es mejor ahorrar el dinero y comprar Access Point Thin - Básicos. Es importante aclarar que entre las 2 categorías de Puntos de Acceso Robustos y Puntos de Acceso Básico existe evidentemente varias sub-categorías.

1.9.3 Interferencias y ruido

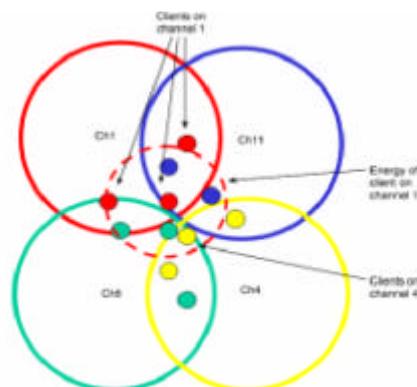
Las interferencias de radio frecuencia son uno de los asuntos más importantes a tener en cuenta para el éxito en el diseño, operación y mantenimiento de sistemas inalámbricos. La principal causa de interferencia en cualquier señal de radio son los materiales del entorno, especialmente aquellos de tipo metálico con tendencia a reflejar las señales. Las fuentes potenciales de interferencia de este tipo son numerosas: materiales metálicos, aislamientos, pinturas de plomo, etc. Y tienden a reducir la calidad de la señal WLAN. Los materiales con alta densidad como el hormigón, tienden a ser más duros de penetrar para las señales de radio, absorbiendo más energía que muchos materiales porosos como madera o yeso.

Los factores de Atenuación e Interferencia de una red inalámbrica wifi 802.11b o 802.11g son:

- ◆ Tipo de construcción
- ◆ Micro-ondas
- ◆ Teléfonos fijos inalámbricos
- ◆ Dispositivos Bluetooth
- ◆ Elementos metálicos como escaleras de emergencia y armarios
- ◆ Peceras
- ◆ Humedad ambiente
- ◆ Tráfico de personas

La lista anterior es válida para el estándar wifi 802.11b y el estándar wifi 802.11g. En cuando al estándar wifi 802.11a, si bien el concepto teórico de obstáculos e interferencias es similar, en la práctica existen varias diferencias, que en general son ventajas. Como se explicó esta tecnología utiliza una banda de frecuencia superior a 5 GHz que aún está muy poco "poblada" o utilizada. Por ejemplo, las interferencias de Micro-ondas, Dispositivos Bluetooth y Teléfonos fijos Inalámbricos, aquí no existen y por lo tanto es más fácil "estabilizar" una red inalámbrica wifi que se base en el estándar wifi 802.11a.

El ruido es otro factor importante a considerar en las comunicaciones inalámbricas, se entiende por ruido a la señal no deseada presente siempre en un sistema eléctrico. El ruido reduce la capacidad del receptor para reconocer correctamente los símbolos, lo que limita la velocidad de transmisión. El ruido se incrementa por una gran variedad de causas, naturales o artificiales. La figura 1.12 muestra la interferencia que se puede provocar entre usuarios.



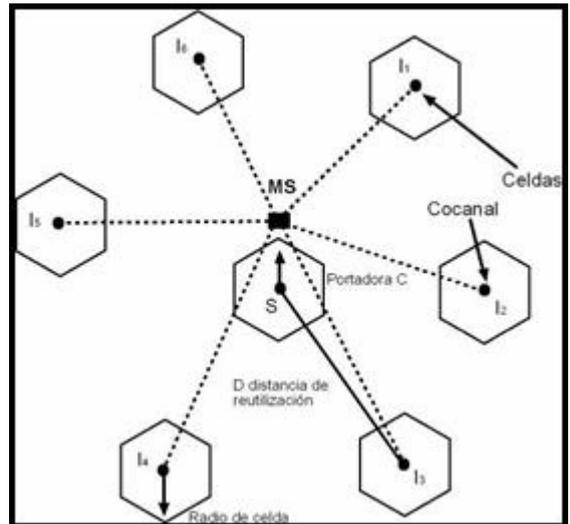


Figura 1.12 Interferencia entre Clientes

Pérdidas de Señal en WIFI. Interferencias y obstáculos

Las ondas de RF transmitidas por las redes inalámbricas WIFI son atenuadas e interferidas por diversos obstáculos y "ruidos". Como comentamos lo que se transmite es energía y esta es absorbida y reducida.

En la figura 1.13, se puede observar un gráfico donde se muestra como en las redes inalámbricas wifi van decreciendo las velocidades de transmisión a medida que nos alejamos del Punto de Acceso Inalámbrico. Esto se debe a que paredes y transmisiones de otros equipos van atenuando la señal. Como se ve en la figura, las velocidades promedio del estándar 802.11b son de 4-5 Mbps y no de 11 Mbps como muchos creen. De la misma manera, las velocidades promedio del estándar Wifi 802.11g son 20-22 Mbps y no 54 Mbps. La velocidad de transmisión de una red inalámbrica wifi, será función de la distancia, los obstáculos y las interferencias.

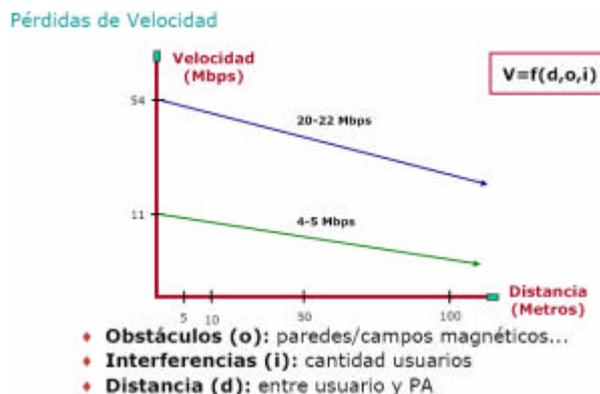


Figura 1.13 Variación de la Velocidad de TX de acuerdo a la distancia.

¹ http://www.tesis.ufm.edu.gt/fisicc/2003/74387/tesis_archivos/image135.jpg

1.10 COBERTURA WLAN INDOOR

Para llevar a cabo un modelo de cobertura WLAN así como para realizar una correcta planificación de su estructura, es importante conocer previamente qué factores pueden intervenir en el proceso completo de intercambio de señales entre emisor y receptor. En general los canales de propagación en interiores (indoor channels) se pueden clasificar en:

- Canales de propagación en Línea de Visión (LOS)
- Canales de propagación en Línea con Obstáculos (OBS)

1.10.1 Límites de Emisión en WLAN

Las autoridades de las telecomunicaciones, entes reguladores y/o controladores limitan la potencia; esta limitación influye evidentemente en la cobertura inalámbrica. En la tabla 1.1 se muestra los niveles de potencia permitidos en cada una de las regiones para la banda de 2.4 GHz.

Máxima potencia de salida	Localización Geográfica	Documento de Complacencia
1000 mW	EE.UU.	FCC 15.247
100 mW (EIRP)	EUROPA	ETS 300-328
10 mW/MHz	JAPÓN	MPT ordinance 79

Tabla 1.1 Niveles de potencia permitidos para cada región

En los Estados Unidos la Comisión Federal de Comunicaciones (FCC) regula el uso de antenas a través de su norma FCC Part 15.247, el cual define los límites de potencia de emisión para redes inalámbricas. En Europa es el “European Telecommunications Standards Institute” que en su documento ETS 300-328 [ETS96] el que regula los límites de potencia de emisión. El concepto básico para la comprensión de estas normas es el EIRP (Equivalent Isotropically Radiated Power), que representa la potencia efectiva máxima de transmisión, incluida la ganancia proporcionada por la antena. Para antenas omnidireccionales el FCC fija el valor máximo de EIRP en 1 vatio.

La banda de 5 GHz ha sido objeto de discusión en la Conferencia Mundial de Radiocomunicaciones, CMR2003. La armonización global del espectro disponible para el uso de WLAN es fundamental en un escenario en el que existen diferencias considerables en cuanto al uso y potencias máximas de transmisión que los distintos países permiten. Como conclusiones de la CMR 2003, se ha resuelto la utilización de las bandas de 5150-5250, 5250-5350 y 5470-5725 MHz para la implementación de sistemas de acceso inalámbrico, incluidas las redes radioeléctricas de área local (WLAN). En la tabla 1.2 se muestran estos valores.

País \ MHz	5150-5250	5250-5350	5470-5725	5725-5875
USA	50 mW interior	250 mW interior/exterior	No permitida	1 W interior/exterior en 5725-5825
Australia	200 mW interior	200 mW interior	No permitida	1 W interior/exterior
Francia	200 mW interior	200 mW / 100 mW (Con / Sin DFS) interior	No permitida	No permitida
Alemania	200 mW interior	200 mW	1 W	No permitida
Reino Unido	200 mW interior	200 mW interior	1 W interior/exterior	En discusión
Países escandinavos	200 mW	200 mW	1 W	No permitida
España	200 mW / 120 mW (Con / Sin DFS) interior	200mW interior	1 W interior/exterior	No permitida

1

Tabla 1.2 Valores de potencia para la banda de 5 GHz

1.10.2 Umbral mínimo de recepción

El umbral mínimo de recepción de un dispositivo va a estar en función de sus características funcionales. La mayoría de los fabricantes incluyen en las especificaciones técnicas de sus productos los niveles de sensibilidad de recepción para cada una de las velocidades definidas en el 802.11b.

1.10.3 Propagación de ondas radioeléctricas indoor

A continuación se procede a describir los fenómenos más relevantes para el modelado de la propagación en entornos indoor, que como hemos comentado anteriormente, tiene características especiales.

1.10.3.1 Propagación en espacio libre (LOS)

Se denomina propagación en espacio libre a la propagación cuando no existen obstáculos en el camino entre el transmisor y el receptor. La pérdida de señal que se produce está en función principalmente de la distancia que les separa, interviniendo igualmente otros factores como el tipo y diseño de las antenas, su patrón de radiación, etc. La transmisión se ve afectada también por posibles reflexiones de la señal que se agregan a la señal directa produciendo variaciones considerables como se verá también en la propagación con línea de obstáculos.

1.10.3.2 Propagación en Línea con Obstáculos (NLOS)

En un entorno cerrado existirán multitud de obstáculos que se interpondrán en el trayecto seguido por las ondas electromagnéticas. Cada uno de estos obstáculos (paredes, suelos, muebles,...) afecta a la señal de determinada forma.

- Los objetos metálicos reflejan las señales de radio. Esto significa que la señal no atravesará muros metálicos y que los objetos metálicos dentro de una habitación reflejarán la señal y causarán desvanecimientos y atenuaciones de la señal.

¹ <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

- Madera, cristal, plástico y ladrillo reflejan parte de la señal de radio y dejan pasar parte del resto.
- Los objetos que contienen un alto grado de humedad absorben la mayor parte de la señal.

Cuando la señal electromagnética se propaga por una estancia es afectada por múltiples fenómenos diferentes debido a los diferentes tipos de obstáculos descritos. Es por tanto imprescindible tener en cuenta estos fenómenos, que causan atenuaciones y desvanecimientos de la señal original, a la hora de diseñar un modelo matemático de cobertura para WLAN.

CAPÍTULO 2

REQUERIMIENTOS PARA IMPLEMENTAR UN MODELO DE COBERTURA Y PROPAGACIÓN EN WLAN

2.1 OBJETIVO Y TIPO DE MODELO

El objetivo principal de un modelo es permitir obtener el nivel de cobertura para poder seleccionar la ubicación óptima de puntos de acceso inalámbricos en el interior de un edificio. Los edificios pueden tener varias plantas y varias habitaciones o salas en cada planta. El modelo permitirá al usuario comprobar la cobertura que se obtendría a partir de la ubicación de ciertos puntos de acceso.

Se utilizará un modelo matemático de cobertura en redes inalámbricas, que tenga en cuenta todos los fenómenos que influyen en la transmisión de señales de radiofrecuencia, implícita o explícitamente; para luego de los cálculos correspondientes generalizarlo.

Para determinar la propagación en el interior, se puede utilizar alguno (o más de uno) de los modelos de propagación en línea de visión (LOS) INDOOR. Estos modelos de propagación pueden ser teóricos o empíricos.

El modelo resultante del presente estudio podrá ser aplicado a entornos reales (edificios existentes) para determinar niveles de cobertura a partir de puntos de acceso dispuestos en el recinto; o para encontrar la situación óptima de colocación de los nuevos puntos de acceso.

Se deben obtener características especiales de los materiales que forman el recinto (atenuación al ser atravesados, coeficiente de reflexión, etc.), los parámetros adecuados para el modelo de propagación en LOS utilizado, y cualquier otra información necesaria.

2.2 USO DE LA RADIOSIDAD

El núcleo del modelo que se pretende obtener, se basa en la forma de calcular la energía que llega a cada punto del entorno.

El modelo de radiosidad es un método para la descripción de reflexiones difusas. Se utiliza en representación realista de imágenes, y se basa en la ley de conservación de la energía. En este método, las transferencias de energía radiante de cada cara deben estar sujetas a las leyes de conservación de la energía.

La energía que ha radiado cada antena en un momento dado, debe permanecer constante, y por lo tanto se debe repartir entre todos los puntos del modelo geométrico tridimensional. Cada superficie a la que le llega señal, se debe comportar como un emisor de una parte de la energía recibida; por lo que el sistema deberá realizar cálculos de energía emitida iterativos. Se debe establecer una condición de parada basada en que las variaciones de energía en cada iteración no sobrepasen un límite.

2.3 MODELOS DE PROPAGACIÓN INDOOR

Un modelo de propagación es un conjunto de expresiones matemáticas, diagramas y algoritmos utilizados para representar las características de radio de un determinado entorno.

La señal emitida por una antena TX va a experimentar múltiples transformaciones en su señal y camino a lo largo de su trayectoria por el medio de propagación, llegando al receptor RX solo una pequeña parte. El camino entre receptor y emisor pueden variar en múltiples formas debido a la existencia de diferentes obstáculos. Esto hace muy difícil predecir la señal recibida en un determinado punto o analizar el canal de radio.

Los modelos de propagación se han enfocado tradicionalmente en predecir la potencia promedio de la señal recibida; así como la variación de la potencia en la proximidad espacial de un lugar en particular.

Los modelos de propagación de radio se pueden clasificar en dos tipos principales: modelos outdoor y modelos indoor. Existen mayor número de modelos de propagación para sistemas inalámbricos outdoor, debido a que la comunicación inalámbrica outdoor se viene utilizando desde hace mucho más tiempo. Los modelos outdoor no tienen en cuenta las características particulares de la propagación indoor.

La mayoría de los modelos de cobertura de redes inalámbricas existentes son modelos de caja negra, en los que se ajustan los parámetros del modelo y se aplican las fórmulas directamente para obtener los resultados de cobertura.

Los resultados de la predicción de cobertura de un Access Point proporcionada por un modelo son muy importantes para facilitar las siguientes tareas:

- Predecir el tamaño de las áreas que se pueden cubrir con un único Access Point.
- Planificar la ubicación de las celdas de modo que, aún utilizando la misma frecuencia, no se interfieran ni causen errores.

En entornos cerrados los niveles de señal fluctúan en mayor medida que en entornos abiertos. Esta diferencia se explica en el hecho de que en una localización específica, el campo eléctrico se forma por un número mucho mayor de componentes indirectos que en el caso de un entorno abierto. Los modelos de propagación indoor difieren de los modelos de propagación tradicionales en dos aspectos:

- Las distancias cubiertas son mucho más pequeñas.
- El componente variable del entorno es mucho mayor para separaciones más pequeñas entre transmisor y receptor.

2.4 MODELOS EMPÍRICOS DE PROPAGACIÓN DE ONDAS ELECTROMAGNÉTICAS

Los modelos empíricos se basan en la extrapolación estadística de resultados a partir de medidas realizadas sobre el terreno. Las influencias propias del entorno son tenidas en cuenta de manera implícita en su conjunto, sin ser reconocidas cada una de ellas de manera aislada., siendo ésta la principal ventaja de estos modelos. Por el contrario, su precisión depende no solo de la precisión de las medidas sino de la similitud entre el entorno donde fueron llevadas a cabo las medidas y el entorno a analizar.

2.4.1 Modelo de Propagación en el Espacio Libre

En el espacio libre, la energía radiada por una antena omnidireccional se propaga por la superficie de una esfera, figura 2.1. El área de la superficie de una esfera de radio d es $(4\pi d^2)$.

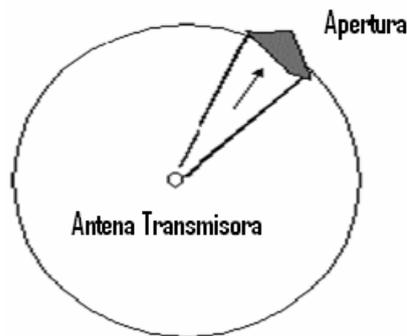


Figura 2.1. Apertura en una antena

El Modelo de Propagación en el espacio libre se utiliza para predecir la potencia de la señal cuando entre el transmisor y el receptor existe una clara línea de vista. Los sistemas de comunicación por satélite y los enlaces microondas se pueden modelar como propagación en el espacio libre.

Como la mayoría de los modelos de propagación a gran escala, el modelo del espacio libre predice que la potencia recibida decae como función de la distancia de separación entre el transmisor y receptor elevada a alguna potencia. La potencia recibida en el espacio libre por una antena receptora, la cual está separada de la antena transmisora una distancia d , está dada por la ecuación de Friis:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}$$

¹ <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

Donde:

- Pr (d) =potencia recibida; la cual es función de la separación Transmisión - Recepción
 Pt =potencia transmitida
 Gt =ganancia de antena transmisora
 Gr =ganancia de la antena receptora
 ? =longitud de onda en metros
 d =la distancia de separación de Transmisión y recepción en metros
 L =pérdidas del sistema no achacables a la propagación

La ganancia de la antena está dada por:

$$G = \frac{4\pi A_e}{\lambda^2}$$

La apertura efectiva A_e se relaciona con el tamaño físico de la antena y con la frecuencia de la portadora mediante:

$$\lambda = \frac{c}{f} = \frac{2\pi c}{\omega_c}$$

Donde:

- F =frecuencia de la portadora (Hz)
 ω_c =frecuencia de la portadora (radianes por segundo)
 c =velocidad de la luz (metros/segundo)

Los valores de R y P_r deben ser expresados en las mismas unidades, y G y G_r son cantidades adimensionales. Las pérdidas L son usualmente debidas a la atenuación de la línea de transmisión, a las pérdidas por filtros, y a las pérdidas de la antena en los sistemas de comunicación. Cuando L=1 significa que no hay pérdidas en el sistema. Las pérdidas por trayectoria representan la atenuación de la señal como una cantidad positiva medida en dB, y se definen como la diferencia entre la potencia radiada efectiva y la potencia recibida. Puede o no incluir el efecto de ganancia de las antenas; cuando se incluyen la ecuación es la siguiente:

$$PL(dB) = 10 \cdot \log \left(\frac{P_t}{P_r} \right) = -10 \cdot \log \left(\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2} \right)$$

Cuando la ganancia de las antenas es excluida, se asume que tiene ganancia unitaria y la ecuación se convierte en:

$$PL(dB) = 10 \cdot \log \left(\frac{P_t}{P_r} \right) = -10 \cdot \log \left(\frac{\lambda^2}{(4\pi)^2 d^2} \right)$$

La ecuación de Friis muestra que la potencia de la señal recibida se atenúa de acuerdo al cuadrado de la distancia entre el transmisor y el receptor, lo que implica que decae 20 dB/década. Cuando se conoce la potencia recibida en una distancia de referencia d_0 , la ecuación siguiente puede utilizarse para calcular la potencia recibida en una distancia más lejana:

$$P_r(d) = P_r(d_0) + 20 \log(d_0/d)$$

La misma ecuación expresada como pérdida de trayecto sería:

$$PL(d) = PL(d_0) + 20 \log(d/d_0)$$

La ecuación de Friis sólo es válida para predecir P_r para valores de d que estén en la región conocida como far-field de la antena transmisora. La región far-field o región de Fraunhofer de una antena transmisora se define como la distancia más allá de la distancia d_f , la cual se relaciona con la dimensión mayor de la apertura numérica de la antena transmisora y con la longitud de onda de la portadora. La distancia de Fraunhofer está dada por:

$$d_f = \frac{2 \cdot D^2}{\lambda}$$

Donde:

D = dimensión física mayor de la antena.

Adicionalmente para estar en la región far-field se debe satisfacer $d \gg D$ y $d \gg \lambda$. Además queda claro que la ecuación no es válida para $d=0$.

2.4.2 Log-Normal Shadowing Path Loss Model

La mayor parte de los modelos empíricos se basan en el siguiente modelo; para el cual, las pérdidas en entornos cerrados se pueden expresar según una ecuación en función de la distancia entre transmisor y receptor como:

$$PL(d) = PL(d_0) + 10n \log(d/d_0) + X_\sigma$$

Donde:

N = variable de pérdida de trayecto

$PL(d_0)$ = pérdida a distancia cercana de referencia

X_s = desviación típica

La variable n es de pérdida de trayecto que depende del tipo de entorno. La tabla 2.1 muestra los valores típicos de n para diferentes entornos. X_s es una variable aleatoria expresada en dB que indica una desviación típica de s dB. $PL(d_0)$ se calcula utilizando el modelo de propagación en espacios abiertos o realizando medidas de campo.

Entorno	N
Edificios (condiciones de visión directa)	1.6 a 2
Edificios (sin visión directa)	2 a 4
Edificios (sin visión directa, separación de uno a tres pisos)	4 a 6

Tabla 2.1 Variable de pérdida de trayecto

La figura 2.2 muestra las curvas de pérdida de trayecto para diferentes valores de la variable de pérdida de trayecto (n).

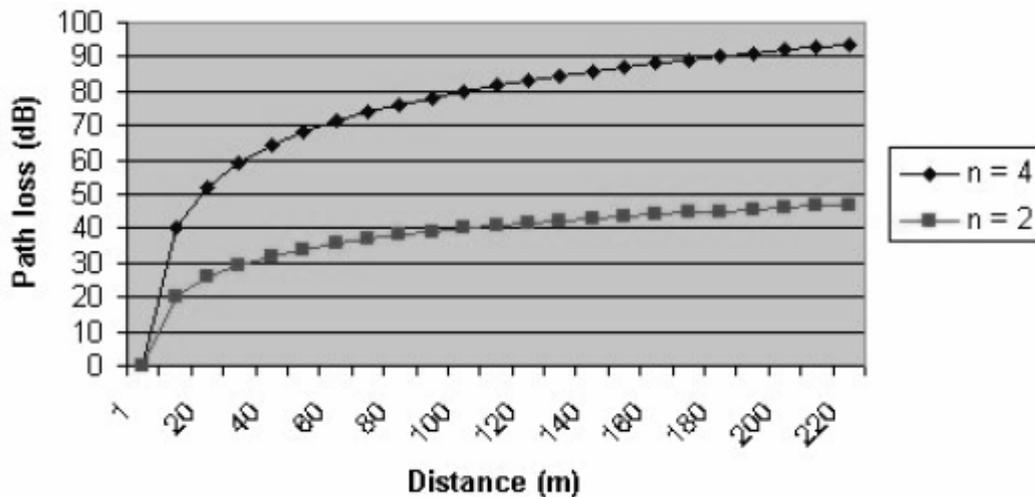


Figura 2.2 Pérdidas de trayecto para diferentes valores de n

Este modelo es una técnica de estimación de pérdidas de propagación muy práctica y que tiene como principal ventaja que considera todos los factores que influyen en la propagación.

2.4.3 Modelo de Pérdida de Trayecto basado en COST 231

Este es el modelo de propagación indoor utilizado en UMTS (Universal Mobile Telecommunications System).

El modelo se basa en el modelo COST 231 definido como:

$$L = L_{FS} + L_c + \sum k_{wi} L_{wi} + n^{((n+2)/(n+1) - b)} * L_f$$

Donde

- L_{FS} = pérdida en espacio libre entre transmisor y receptor
- L_c = constante de pérdida; se fija normalmente en 37 dB.
- K_{wi} = número de paredes de tipo i penetradas
- n = número de suelos penetrados
- L_{wi} = pérdida debida a muro de tipo i
- L_f = pérdida entre suelos adyacentes
- b = parámetro empírico

En la tabla 2.2 se muestran los valores para: pérdida entre suelos adyacentes, pérdida debida a muro de tipo i.

Tipo de Pérdida	Descripción	Factor (dB)
L_f	Suelos (estructura típica) - Baldosas - Revestimiento de hormigón - Espesor típico < 30 cm	18.3
L_{w1}	Muros internos finos - Yeso - Muros con muchos huecos (ventanas)	3.4
L_{w2}	Muros internos - Hormigón, ladrillos - Mínimo número de huecos	6.9

Tabla 2.2 Valores de pérdida para suelos y muros

El modelo COST 231 es un modelo empírico que tiene en cuenta las pérdidas de propagación en espacio abierto así como las pérdidas introducidas por las paredes, suelos y techos penetrados en el trayecto directo entre transmisor y receptor.

2.4.4 Modelo basado en el número de muros y suelos (simplificado)

Caracteriza la pérdida de trayecto en interior por un exponente fijo de 2 (como en el espacio libre) y unos factores de pérdida relacionados con el número de suelos y muros que atraviesa la línea recta entre emisor y receptor.

$$L = L_1 + 20\log(r) + n_f a_f + n_w a_w$$

Donde

- r = distancia en metros en línea recta
- L_1 = pérdida de referencia con $r=1$ metro
- a_f = atenuación por cada suelo que atraviesa

a_w = atenuación por cada muro que atraviesa
 n_f = número de suelos que atraviesa
 n_w = número de muros que atraviesa

2.4.5 Modelo UIT-R (Unión Internacional de Telecomunicaciones)

Es similar a los anteriores pero sólo tiene en cuenta explícitamente el número de suelos. Las pérdidas en el mismo piso por atravesar muros, se incluyen implícitamente cambiando el exponente en la pérdida de trayecto.

$$L_T = L_1 + 20\text{Log}_{10}(f_c[\text{MHz}]) + 10\text{Log}_{10}(r[m]) + L_f n_f - 28$$

2.4.6 Modelo de Atenuación lineal de la trayectoria (Linear Path Attenuation Model)

Para un transmisor y un receptor que se encuentran en la misma planta, Andelman propuso el “*Linear path attenuation model*”. El path loss medido en dB se obtiene del path loss en espacio libre, más un factor que es lineal del rango que experimentalmente se ha obtenido. La fórmula utilizada en este modelo es:

$$PL(d) = PL_{FS} + ad$$

Dónde a es el coeficiente de atenuación lineal y d es la distancia entre transmisor y receptor. En el caso de un ambiente de oficinas, el coeficiente a sería 0.47 dB/m. Este modelo es bastante más simple que el modelo Log-Normal Shadowing Path Loss, y no tiene en consideración efectos de desvanecimiento. Sólo toma en consideración la pérdida en espacio libre. Este modelo es susceptible de ser específico de un sitio, esto es debido a que el valor de a varía de un entorno a otro y debe ser medido con precisión para poder demostrar los beneficios de este modelo.

2.5 MODELOS TEÓRICOS DE PROPAGACIÓN DE ONDAS ELECTROMAGNÉTICAS

Se basan en principios fundamentales de la física en cuanto a propagación de ondas de radio y los fenómenos que la rodean. Pueden ser aplicados en diferentes entornos sin afectarles a su precisión.

Los algoritmos usados por los modelos deterministas son generalmente muy complejos y poco eficientes. Por esta razón su implementación se restringe a pequeñas áreas. Por el contrario, si su implementación es correcta, proporcionan gran precisión en su predicción comparados con los modelos empíricos. En la actualidad existen diferentes modelos teóricos siendo los más populares los basados en Ray-tracing y FDTD (Finite-Difference Time-Domain).

2.5.1 Modelos basados en Ray-Tracing

El algoritmo de ray-tracing calcula todos los posibles caminos desde el transmisor al receptor. En los modelos básicos de ray-tracing, la predicción se basa en cálculos de transmisión en espacio abierto complementados con el efecto de reflexión de las paredes, teniendo en cuenta una única reflexión. Los algoritmos de ray-tracing más complejos incluyen mecanismos de difracción, dispersión difusa y penetración a través de diversos materiales. En conclusión, el nivel de señal en un punto determinado se obtiene mediante la suma de los componentes de todos los caminos posibles existentes entre transmisor y receptor. Además de las pérdidas de propagación, en estos modelos se pueden predecir de manera fiable la dispersión en el tiempo de la señal. Hoy en día los modelos de ray-tracing están considerados entre los más precisos de entre los modelos de predicción de potencia de campo; sin embargo, requieren una representación muy detallada del área a analizar. La precisión del modelo depende en gran medida de la precisión y completitud/complejidad de la base de datos asociada a la representación. Por otro lado, el tiempo de computación depende en modo exponencial de estos detalles. Así, el tiempo de computación de un área reducida pero muy detallada puede ser mucho mayor que el de un área mayor pero con menor nivel de detalle.

2.5.2 Modelos FDTD (Finite-Difference Time-Domain)

Las características de la propagación de radio se pueden derivar resolviendo directamente las ecuaciones de Maxwell relativas a propagación de ondas electromagnéticas. El método FDTD (Finite-Difference Time-Domain) es probablemente el método más utilizado para la obtención de una solución numérica de las ecuaciones de Maxwell. En este método las ecuaciones de Maxwell se aproximan por medio de un conjunto finito de ecuaciones diferenciales. Antes de realizar los cálculos es necesario definir una cuadrícula específica (regular o irregular) sobre el área de interés. Una vez que estas condiciones iniciales han sido definidas, el algoritmo FDTD emplea las diferencias centrales para aproximar las derivadas tanto en el espacio como en el tiempo. En los nodos de la cuadrícula la solución se determina iterativamente, resolviéndose de este modo las ecuaciones de Maxwell directamente.

Al igual que los modelos basados en ray-tracing, los modelos FDTD son muy exigentes computacionalmente. El tiempo de computación depende proporcionalmente del tamaño del área a ser analizada, pero no significativamente de los detalles incluidos en su descripción. Sin embargo el número de nodos de la cuadrícula está exponencialmente relacionado al tamaño del área y la frecuencia de operación. La precisión del modelo FDTD es comparable a la de los modelos basados en ray-tracing; y la predicción es tan precisa como pueda serlo la base de datos de descripción del área.

Debido a su complejidad computacional, los modelos FDTD son aconsejables sólo en tareas de predicción de campo en pequeñas áreas. Para áreas de mayor tamaño los modelos de ray-tracing son más aconsejables.

2.6 PROPAGACIÓN EN LÍNEA CON OBSTÁCULOS (NLOS)

El entorno normal bajo el cual coexisten las WLAN, en algunos casos es cerrado y se presentan multitud de obstáculos que se interpondrán en el trayecto seguido por las ondas electromagnéticas. Cada uno de estos obstáculos (paredes, suelos, muebles,...) afecta a la señal de determinada forma. Entre los principales obstáculos se consideran:

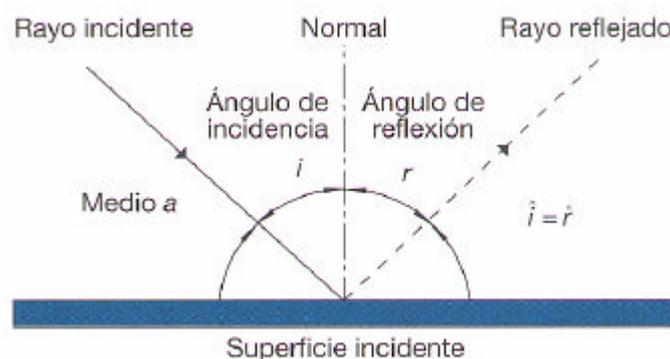
- Los objetos metálicos reflejan las señales de radio. Esto significa que la señal no atravesará muros metálicos y que los objetos metálicos dentro de una habitación reflejarán la señal y causarán desvanecimientos y atenuaciones de la señal.
- Madera, cristal, plástico y ladrillo reflejan parte de la señal de radio y dejan pasar parte del resto.
- Los objetos que contienen un alto grado de humedad absorben la mayor parte de la señal.

Cuando la señal electromagnética se propaga por un recinto es afectada por múltiples fenómenos diferentes debido a los diferentes tipos de obstáculos descritos. Es por tanto imprescindible tener en cuenta estos fenómenos, que causan atenuaciones y desvanecimientos de la señal original, a la hora de diseñar un modelo matemático de cobertura para WLAN

2.6.1 Reflexión

La reflexión ocurre cuando una onda electromagnética que se propaga por el aire incide contra un objeto de grandes dimensiones en comparación con la longitud de onda de la señal. El resultado puede ser que la señal sea absorbida, reflejada o una combinación de ambas. Esta reacción depende principalmente de:

- Propiedades físicas del obstáculo, como pueden ser su geometría, textura y composición.
- Propiedades de la señal, como el ángulo de incidencia, orientación y longitud de onda.



1

Figura 2.3 Reflexión de una señal

¹ html.rincondelvago.com/ondas-y-acustica.html

Un conductor perfecto refleja la totalidad de la señal. Otros materiales reflejan solo una parte de la energía incidente y transmiten el resto. La cantidad exacta de transmisión y reflexión de la señal depende igualmente del ángulo de incidencia así como del grosor y propiedades dieléctricas material.

2.6.1.1 Desvanecimiento por multitrayecto debido a reflexiones

Cuando una señal electromagnética es transmitida por el aire, es muy probable que debido al fenómeno de reflexión, alcance al receptor por múltiples trayectos. Las señales procedentes de caminos alternativos llegarán ligeramente retardadas con respecto a la señal directa, lo que provoca efecto de desvanecimiento. Esto es debido a que las señales reflejadas tendrán diferente amplitud que la señal directa cuando lleguen al punto de recepción retardadas.

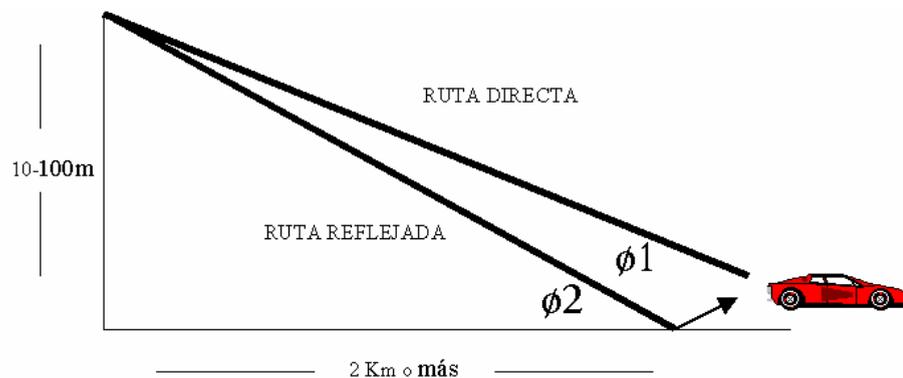


Figura 2.4 Desvanecimiento por Multitrayecto

El Multitrayecto provoca variaciones aleatorias en la amplitud de la señal recibida sobre un margen de frecuencias. Sus efectos varían dependiendo de la localización de la antena así como del tipo de antena utilizada.

2.6.1.2 Perfil de retardo

El perfil de retardo es la previsión de potencia recibida por unidad de tiempo con un cierto nivel de retardo. El MDT (*Maximum Delay Time Spread*) es el intervalo de tiempo total durante el que se reciben señales reflejadas con energía significativa. El RMS (*Root Mean Square Delay Spread*) es la desviación típica del retardo de reflexión, ponderado según la energía de las ondas reflejadas.

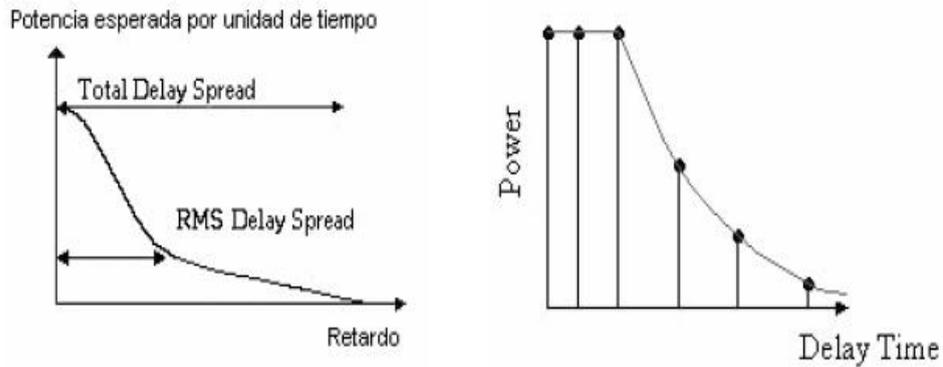


Figura 2.5 Perfil de retardo

El perfil de retardo típico tiene una forma plana en su cabeza hasta un determinado punto cayendo posteriormente con el tiempo a niveles cada vez más débiles. Esto es debido a que las primeras señales reflejadas se reciben con potencia casi idéntica.

2.6.2 Penetración

La penetración se produce cuando la señal se encuentra en su camino con un obstáculo que es, aparentemente, transparente para las ondas de radio. Cuando la señal penetra un obstáculo experimentará una pérdida, la cual será función del grosor del objeto y del material del que está compuesto. La frecuencia de la onda electromagnética también influye en qué proporción de la señal incidente atraviesa el objeto. Existen multitud de estudios sobre pérdidas estimadas en diferentes materiales en WLAN. La tabla es un extracto del documento publicado por Ericsson “Wireless LAN User’s Guide Versión 4.2” y en ella se presentan las pérdidas predecibles en la penetración de diferentes tipos de materiales.

TIPO DE OBSTÁCULO	PERDIDA
Espacio abierto	0 dB
Ventana (tintado no metálico)	3 dB
Ventana (tintado metálico)	5-8 dB
Muros finos	5-8 dB
Muros medios de madera	10 dB
Muros gruesos	15-20 dB
Muros muy gruesos	20-25 dB
Suelo/Techo grueso	15-20 dB
Suelo/Techo muy grueso	20-25 dB

Tabla 2.3 Penetración en diferentes tipos de materiales

¹ <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

2.6.3 Difracción

La difracción es la desviación del rayo luminoso al rozar el borde de un cuerpo opaco. Las ondas difractadas se forman cuando el camino de propagación de la onda de radio es obstruido por una superficie que tiene irregularidades o bordes puntiagudos o angulados. La difracción ocurre cuando los obstáculos son impenetrables por las ondas de radio. Basándose en el principio de Huygen, el resultado son ondas secundarias alrededor y detrás del obstáculo, figura, incluso en zonas sin visibilidad directa entre transmisor y receptor.

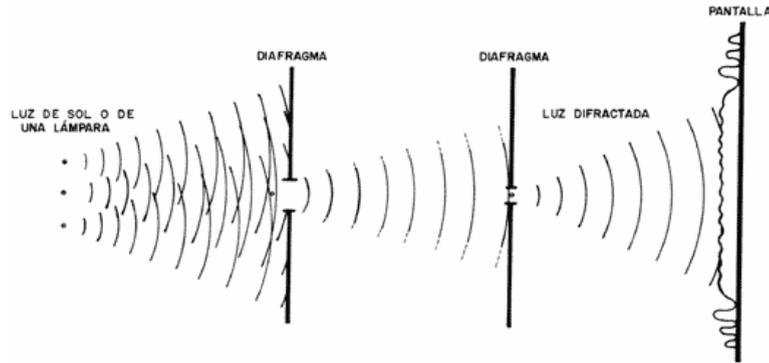


Figura 2.6 Difracción de una señal

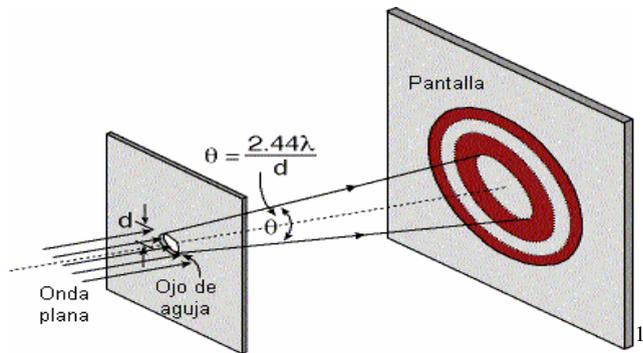


Figura 2.6.1 Difracción de una señal

2.6.4 Dispersión

La dispersión ocurre cuando en el camino la señal se encuentra con objetos cuyas dimensiones son pequeñas con relación a la longitud de onda. El resultado es que el frente de onda se rompe o dispersa en múltiples direcciones. En la figura se observa el fenómeno.

¹ www.difo.uah.es/curso/c03/cap03.html

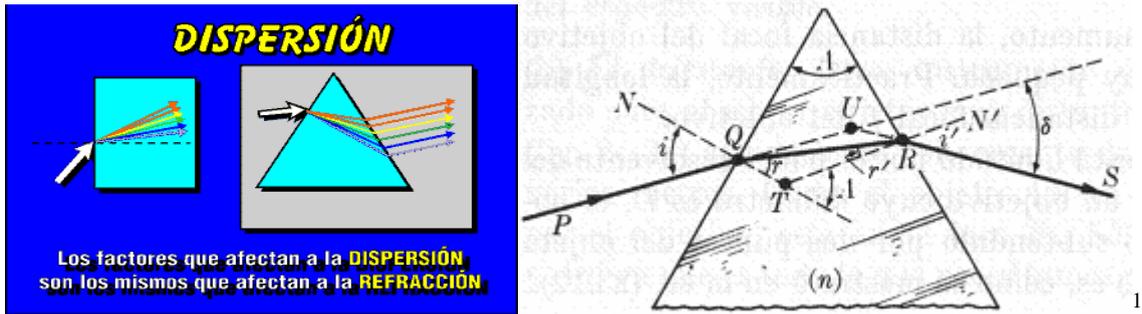


Figura 2.7 Efecto de dispersión de una señal

Las ondas dispersas son producidas por superficies desiguales, pequeños objetos y otras irregularidades. La mayoría de las construcciones modernas contienen vigas de hierro forjado en su estructura además de conductos para los servicios eléctricos y de tuberías.

¹ www.difo.uah.es/curso/c03/cap03.html

CAPÍTULO 3

ANÁLISIS DE LA RED ACTUAL Y DISEÑO DEL MODELO

3.1 ANTECEDENTES

El modelo escogido para el cálculo de la pérdida de la señal por la propagación del aire es el **Modelo de Propagación Log-Normal Shadowing Path Loss Model** se escogió este modelo debido a que para su cálculo se basa en tomas reales de campo para sacar un factor de pérdida general. Los valores se pueden obtener ya que actualmente la Universidad del Azuay cuenta con 26 puntos de acceso (**croquis del anexo 1**) en su campus por lo que los valores obtenidos se asemejarán en gran medida a la realidad. En el plano se observara la ubicación de los Access Point pero no su totalidad ya que como los edificios tienen varias plantas, se vera uno por edificio.

Estos puntos de acceso han sido colocados en forma empírica sin ningún estudio de propagación electromagnética. Con el presente trabajo se pretende obtener un plan a seguir ya sea en ampliaciones a la red Wlan de la Universidad del Azuay así como también a la implementación de servicios como Voz IP sobre dicha red.

Los pasos que se relatan a continuación son los pasos que se siguieron para obtener el factor de pérdida general para el modelo de propagación Log-Normal Shadowing Path Loss Model.

3.2 ESTRUCTURA DE LA RED ACTUAL

La Universidad del Azuay dispone de varios edificios en su infraestructura, entre ellos tenemos: Facultad de Administración, Facultad de CCTT, Edificio de Investigaciones, Facultad de Filosofía, Biblioteca entre otros. Para tener una cobertura total en los edificios se han implementado access point en diferentes pisos de estos edificios.

Cada uno de los Access Point son conectados a un switch de piso mediante un cable categoría 5e permitiendo la velocidad máxima teórica de 100Mbps, el Access Point podrá manejar hasta 54 Mbps según las normas 802.11b, El acceso de los alumnos es con una asignación de una Ip que es proporcionada mediante un servidor DHCP, en la actualidad existen 865 cuentas creadas (Mayo/2007). Para cumplir con las normas de cableado estructurado ya que las distancias son mayores a 100mts entre edificios y además la necesidad de satisfacer el ancho de banda y velocidad de transferencia de datos entre cada edificio del Campus Universitario, internamente la red tiene su interconexión entre Edificios realizado con cable de Fibra Óptica Multimodo G652 de 6 hilos.

Por esta razón se debe tener en cuenta que la cantidad de información que puede manejar el backbone de la Universidad del Azuay es de 1 Gbps lo que permitirá en un futuro poder manejar tráfico de Imágenes, Videoconferencias, etc.

Se debe aclarar que se tienen algunas áreas de la Red WLAN dentro del campus Universitario que las denominaremos en este estudio así:

AREAS DEL CAMPUS UNIVERSITARIO.

- ◆ Biblioteca.
- ◆ Administración P.B.
- ◆ Administración P1
- ◆ Administración P2
- ◆ Administración P3
- ◆ Administración P4
- ◆ Filosofía PB
- ◆ Filosofía P1
- ◆ Filosofía P2
- ◆ Filosofía P3
- ◆ Filosofía P4
- ◆ Laboratorio de Electrónica
- ◆ Decanato de Investigaciones y Centro de Computo
- ◆ Facultad de Ciencias y Tecnología.
- ◆ Edificio de Administración Central
- ◆ Facultad de Diseño

Equipamiento de la Red

La red se encuentra formada por equipos Access Point Linksys Wireless-G Access Point WAP54G; el cual es un Access Point inalámbrico que opera a 54 Mbps. El mismo presenta las siguientes características:

Generales:

Tipo de dispositivo:	Access Point
Anchura:	18.6 cm.
Profundidad:	20 cm.
Altura:	4.8 cm.
Peso:	482 g
Protocolos Soportados:	802.11g 802.11b

Conexión de redes:

Velocidad de transferencia de datos:	54 Mbps
Banda de frecuencia:	2.4 Ghz
Formato código de línea:	DBPSK, DQPSK, CCK, OFDM
Protocolo de interconexión de datos:	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g
Método de espectro expandido:	OFDM, DSSS
Protocolo de conmutación:	Ethernet
Protocolo de direccionamiento:	Direccionamiento IP estático
Protocolo de gestión remota:	HTTP
Indicadores de estado:	Actividad de enlace, alimentación, Enlace

Cumplimiento de normas: IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g

Antena:

Directividad: Omnidireccional

Interfaces:

- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x red - Radio-Ethernet

Diversos:

Cables (Detalles): 1 x cable de red
Algoritmo de cifrado: WEP de 128 bits, WPA, WPA2
Cumplimiento de normas: CE, IC CS-03, FCC, RoHS
Dispositivo de alimentación: Adaptador de corriente - externa
Sistema operativo requerido: Microsoft Windows 98SE/2000/ME/XP
Detalles de los requisitos del sistema: - 200 MHz - RAM 64 MB
Temperatura mínima de funcionamiento: 0 °C
Temperatura máxima de funcionamiento: 40 °C
Ámbito de humedad de funcionamiento: 10 - 85%

En la figura 3.17 se observa la apariencia física del equipo.



Figura 3.17 Access Point Linksys Wireless-G Access Point WAP54G

3.2.1 Edificio de la Facultad de Administración

Los datos calculados y obtenidos en forma teórica, además de la adquisición manual de datos reales se describen a continuación solo para este Edificio, este procedimiento se realizara para todos los demás sectores de la universidad en donde existen los Access Point.

El edificio tiene varios Access Point en su interior los cuales son conectados a un cuarto de telecomunicaciones existente en el edificio, los Access Point se encuentran en una topología estrella, En la Planta Baja el Access Point tiene su cobertura destinada a la secretaria de la facultad y existe otro AP para la sala de Profesores, Los 4 Access Point restantes del edificio se encuentra en un lugar específico y con igual ubicación en todos

los pisos, la infraestructura física es de idénticas características a sus alrededor, esto se debe tomar en cuenta para poder realizar los cálculos, se debe también aclarar que entre los Access Point no existe un solapamiento de las áreas de cobertura ya que entre pisos existe una losa de gran espesor que no permite el paso de las ondas electromagnéticas.

La ubicación de los Access Point hace preveer una cobertura para un aula específica y daran el acceso a los alumnos en cada piso, pero existe valores de campo validos para poder acceder a la red desde los pasillos y corredores, así también existe lugares donde la señal aunque esta dentro del diámetro de cobertura la señal se atenúa por los muros y paredes internas existentes como se puede ver en el capitulo IV.

Para obtener la situación actual y real de la red WLAN en el Campus de la Universidad del Azuay, se ha realizado un estudio de propagación radioeléctrica y el análisis espectral

En cada uno de los lugares del campus universitario se realizo un barrido del espectro radioeléctrico el cual se lo realizo con un analizador de espectros configurado de manera que recoja mediciones en la frecuencia de trabajo de los Access Point (2,41Ghz).

El analizador nos permite visualizar las componentes espectrales existentes y que están presentes en los diferentes sectores de la Universidad del Azuay. Es muy importante obtener estos valores para analizar diferentes interferencias (cocanal y canal adyacente) que son provocadas por otras portadoras o equipos cercanos de telecomunicaciones que trabajen en la frecuencia que se esta realizando este estudio.

En todo Survey de Frecuencias se debe tener en cuenta 2 aspectos importantes para realizar las mediciones:

- Adquirir los datos con la antena en la polarización vertical tanto como la horizontal,
- Los datos deben ser tomados desde los 0° hasta los 360°, es decir realizar el barrido dando una vuelta completa en el propio eje.

En las siguientes figuras se puede observar que por cada sector de la Universidad existe dos gráficos, uno en polarizacion horizontal y otro en polarizacion vertical, además los datos han sido adquiridos realizando el barrido y están dibujados en un solo grafico. Los análisis espectrales no se realizaron en todos los lugares donde existe access point, como la biblioteca, sino mas bien se dividió en zonas para poderlos observar de manera mas general y no redundar en gráficos que nos darán el mismo resultado.

Para el edificio de Administración en la parte interior se a realizado el barrido de l espectro de frecuencias obteniendo los siguientes resultados.

Valores obtenidos con la antena en Polarización Horizontal a 2.41 GHz. en el edificio de Administración

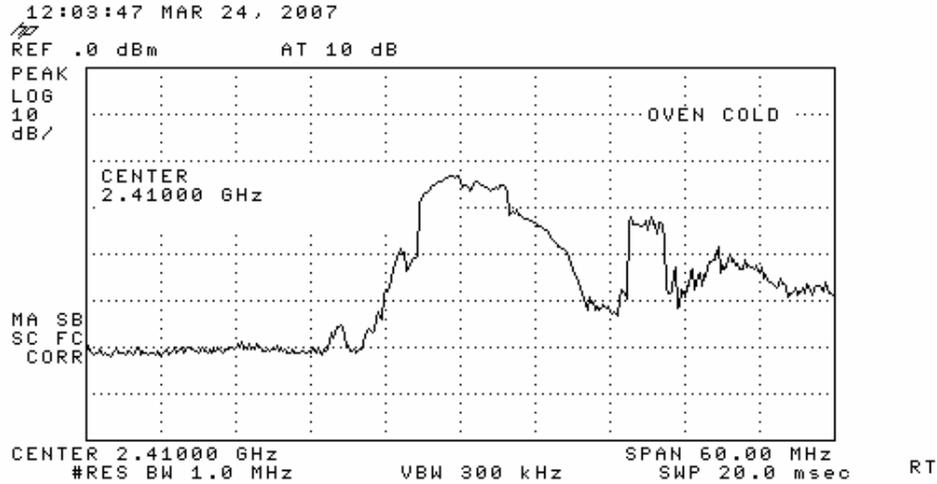


Figura 3.1 Polarización Horizontal

Para la medición se debe tomar en cuenta la frecuencia central y el span (ancho de ventana para la medición). En el grafico se observa que existen portadoras dentro del rango de interés 2.38 GHz a 2.44 GHz. El valor de densidad espectral que se obtiene en la frecuencia central es de -57 dB. El valor de ref. es de 0 lo que indica que para obtener el valor de la medición se contara de 10 en 10 hasta llegar al pico máximo que se vera luego de todo el barrido.

Valores obtenidos con la antena en Polarización Vertical a 2.41 GHz. en el edificio de Administración.

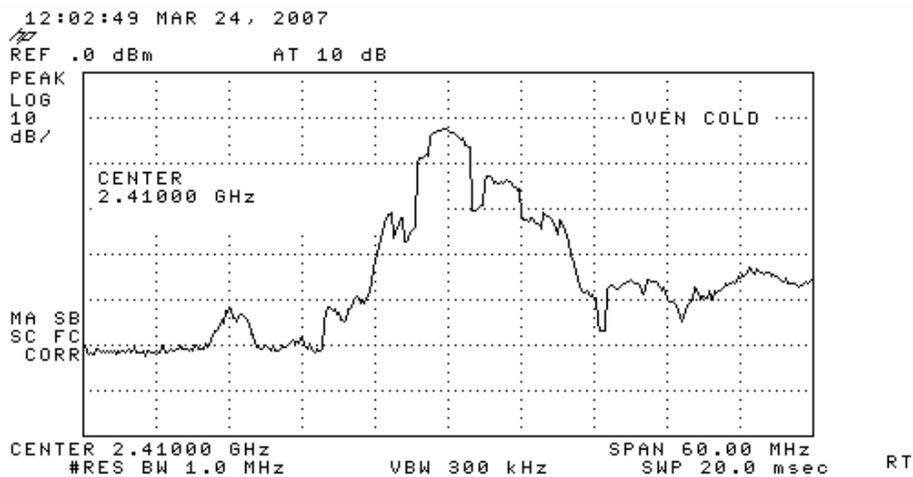


Figura 3.2 Polarización Vertical

En el grafico se observa que dentro del rango analizado, 2.38 GHz a 2.44 GHz se observan múltiples portadoras, igualmente al ser un lugar donde se encuentran trabajando los AP se ve claramente el uso de este espectro, el valor pico de densidad espectral es de -67 dB.

Valores obtenidos con la antena en Polarización Horizontal a 2.437 GHz. en el edificio de Administración

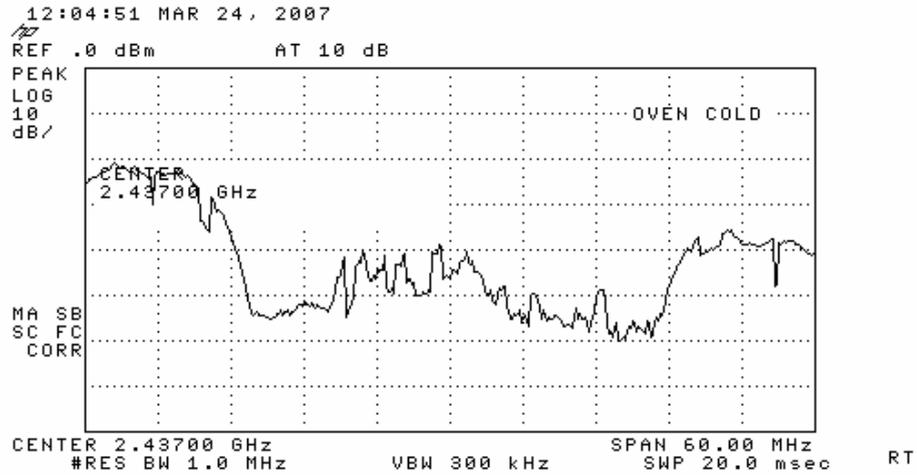


Figura 3.3 Polarización Horizontal

En el grafico se observa que dentro del rango analizado, 2.38 GHz a 2.44 GHz se observan múltiples portadoras, igualmente al ser un lugar donde se encuentran trabajando los AP se ve claramente el uso de este espectro, el valor pico de densidad espectral es de - 27 dB.

Valores obtenidos con la antena en Polarización Vertical a 2.437 GHz. en el edificio de Administración.

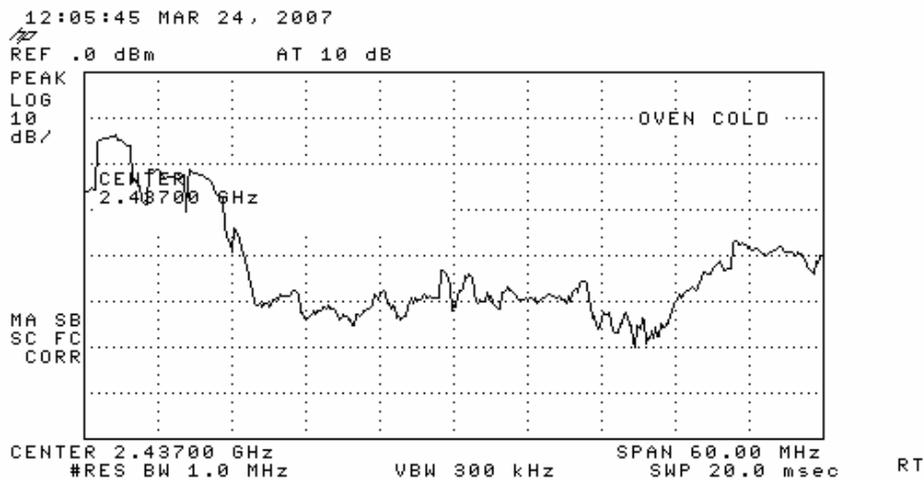


Figura 3.4 Polarización Vertical

En el grafico se observa que dentro del rango analizado, 2.38 GHz a 2.44 GHz se observan múltiples portadoras, el valor pico de densidad espectral es de -29 dB.

3.2.1.1 Procedimiento y Aplicación para los Cálculos

Como se indico anteriormente se procede a realizar un a obtención manual realizando diferentes mediciones de campo en todos los lugares donde se encuentra instalado un Access Point, esta obtención de datos se realizo con un computador portátil marca DELL INSPIRON E1405 utilizando su tarjeta WIFI “Dell Wireless 1390 WLAN Mini-Card” y con el software que permite observar la distancia y la perdida con respecto a un punto fijo que en este caso serán cada uno de los diferentes Access Point, con este equipamiento se recogen los datos que posteriormente serán utilizados para el cálculo, se debe realizar el mismo procedimiento en los diferentes Access Point ubicados en el Campus Universitario. Los datos fueron tomados con una exactitud en distancia, como se podrá ver en los cálculos se ha variado la distancia de metro en metro, se puede observar en algunos casos la perdida de campo un poco pronunciada, entonces esto confirma que los datos serán lo mas aproximados a la realidad existente.

Como se menciona anteriormente para la realización de los cálculos se utilizará el **Modelo de Propagación Log-Normal Shadowing Path Loss Model**, debido a que este utiliza para sus cálculos condiciones reales del entorno y en vista de que ya se dispone de una red Wireless. Este modelo, para su aplicación, requiere de valores de medición tomados en el campo. La fórmula general del modelo indica que para una etapa inicial de cálculo es necesario tomar valores de medición correspondientes a PL (d0) y PR (d). PL (d0) es el valor de potencia recibida en el computador portátil a una distancia de referencia, a la cual se tomó a 1 metro (d0 = 1metro). El valor de PR (d) se mide con el computador portátil a diferentes distancias y en diferentes posiciones con respecto a las radiaciones del Access Point. Los valores de potencia obtenidos mediante el computador se encuentran en dBm y pueden ser aplicados directamente al modelo.

Con las mediciones realizadas se procede, en una primera etapa, a introducir estos valores en el modelo. Para esta etapa de análisis el modelo se reduce a:

$$PR(d) = PL(d_0) + 10 \cdot n \cdot \log_{10} \left(\frac{d}{d_0} \right)$$

Al observar la fórmula se determina que la incógnita a resolver es el valor de la variable de pérdida de trayecto n. Entonces la fórmula se acondiciona de la siguiente forma:

$$n = \frac{PR(d) - PL(d_0)}{10 \cdot \log_{10} \left(\frac{d}{d_0} \right)}$$

Introduciendo los valores de campo y los de las distancias en la fórmula se obtiene el valor de la variable de pérdida del trayecto. Así por ejemplo; en el edificio de Administración Planta Baja, la distancia de referencia d0=1m (este valor será utilizado como referencia en todos los cálculos), a esta distancia de referencia se obtiene en el computador portátil un campo PL (d0) = -35dBm (este valor de PL (d0) será fijo) y una de las mediciones se toma a una distancia d = 3m, con lo cual se obtiene un campo PR (d) = -36 dBm. Con estos valores en la fórmula se obtiene un valor de la variable de pérdida del trayecto n = 0.20959.

Se realizara el mismo procedimiento para el resto de mediciones a las diferentes distancias. En la tabla se muestran los valores de n para las diferentes distancias y mediciones de campo para el interior Administración Planta Baja sobre el AP que sirve a la secretaria, el mismo calculo se realiza para la sala de profesores obteniendo un área de cobertura como se ve en el capitulo VI.

PL(d ₀)	PR(d)	Distancia (d)	n
-35	-36	2	$n= 0,33219281$
-36	-37	3	$n= 0,20959033$
-36	-39	4	$n= 0,49828921$
-36	-41	5	$n= 0,71533828$
-36	-42	6	$n= 0,77105833$
-36	-44	7	$n= 0,94663573$
-36	-45	8	$n= 0,99657843$
-36	-48	9	$n= 1,25754196$
-36	-51	10	$n= 1,50000000$
-36	-53	12	$n= 1,57526829$
-36	-56	13	$n= 1,79542344$
-36	-58	14	$n= 1,91950631$
-36	-61	15	$n= 2,12568538$

Tabla 3.1 Valores de Campo (dBm), Distancia (m) y valor de perdidas

El valor de n es la variable de pérdida de trayecto y depende del tipo de entorno en el que se encuentre instalado el Access Point. Como se observa en la fórmula este valor altera el valor de PR (d) haciéndolo mayor o menor.

Con los valores de n determinados, se procede a encontrar un valor de n medio que se considera como la pérdida de trayecto media para el entorno en análisis. En el caso del ejemplo; n medio = 1,15009697 este valor será tomado para realizar los cálculos de potencia y cobertura de un Access Point en cualquier otro lugar del Campus Universitario o lugar que tenga un medio similar.

Con el valor de n medio ya determinado se procede a introducir un nuevo concepto en la fórmula del modelo. Se utiliza la misma fórmula a la cual se suma un valor de X_s , la misma es una variable aleatoria expresada en dB que indica una desviación típica de s dB, es decir, nos indica cuan alejadas se encuentran las muestras tomadas con respecto a la media.

$$PL(d) = PL(d_0) + 10n \log(d/d_0) + X_s$$

A partir de esta nueva consideración se proceda a calcular el valor de X_s despejando de la fórmula.

Se obtienen los siguientes valores:

<i>n</i>	<i>Xs</i>
<i>n</i> = 0,33219281	2,39078068
<i>n</i> = 0,20959033	4,37426023
<i>n</i> = 0,49828921	3,78156137
<i>n</i> = 0,71533828	2,87314893
<i>n</i> = 0,77105833	2,76504092
<i>n</i> = 0,94663573	1,51912484
<i>n</i> = 0,99657843	1,17234205
<i>n</i> = 1,25754196	-1,25147953
<i>n</i> = 1,50000000	-3,73607038
<i>n</i> = 1,57526829	-4,84417840
<i>n</i> = 1,79542344	-7,45262048
<i>n</i> = 1,91950631	-9,09009447
<i>n</i> = 2,12568538	-11,75259083

Tabla 3.2. Valores de Pérdidas y *Xs*

El propósito de obtener la variable aleatoria *Xs*, es poder tener una variación en el espacio muestral tomado en el campo, para a partir de esta poder determinar una varianza con las muestras o mediciones. En teoría de probabilidad y estadística la varianza es un estimador de la dispersión de una variable aleatoria con respecto a su media. Conociendo la varianza se puede determinar la desviación estándar

Para conocer con detalle un conjunto de datos, no basta con conocer las medidas de tendencia central, (*n* media en este caso) sino que necesitamos conocer también la desviación que representan los datos en su distribución, con objeto de tener una visión de los mismos más afín.

La desviación estándar o desviación típica es una medida de dispersión para variables de razón y de intervalo, de gran utilidad en la estadística descriptiva. Se trata de una medida cuadrática de lo que se apartan los datos de su media, y por tanto, se mide en las mismas unidades que la variable.

La desviación estándar se calcula mediante la raíz cuadrada de la varianza. Para el ejemplo del Edificio de Administración se tiene:

VARIANZA =	28,79257487
DESVIACION =	5,36587131

Tabla 3.3 Valores de Perdidas y *Xs*

Este valor de desviación típica, de todas las muestras, que se obtiene es un valor aleatorio que se sumará a la fórmula como el nuevo X_s .

Para realizar la generalización de las pérdidas de trayecto en un determinado Access Point de La Universidad del Azuay se introduce el valor de n medio y se suma el valor de desviación calculado. De esta forma se determinan las pérdidas en el trayecto. La medida aleatoria permite simular variaciones de señal causadas por el entorno radioeléctrico. Aunque la señal de cobertura sea aleatoria, nos da una indicación de las variaciones de señal que se producen en las zonas donde la desviación es significativa respecto al resto de la señal.

Cobertura de la Señal

En este modelo de propagación se han tomado valores reales de campo en las diferentes zonas, se debe además saber que la cobertura a variado en cada ángulo de 0 a 360°, por paredes y obstáculos en la zona de cobertura, para los cálculos fue desarrollado con un valor de campo hacia un ángulo específico que fue los 90°, para el dibujo del área de cobertura se a tomado una radiación omnidireccional pero que variara de acuerdo a los obstáculos que se pueden ver en el capítulo II y IV.

3.2.2 Edificio de Administración Central

Los resultados obtenidos del análisis espectral para este sector de la Universidad, se encuentran desarrollados a continuación y se refiere además a los sectores de la *Biblioteca y Decanato de Investigaciones y centro de Computo*.

Valores obtenidos con la antena en Polarización Horizontal a 2.41 GHz.

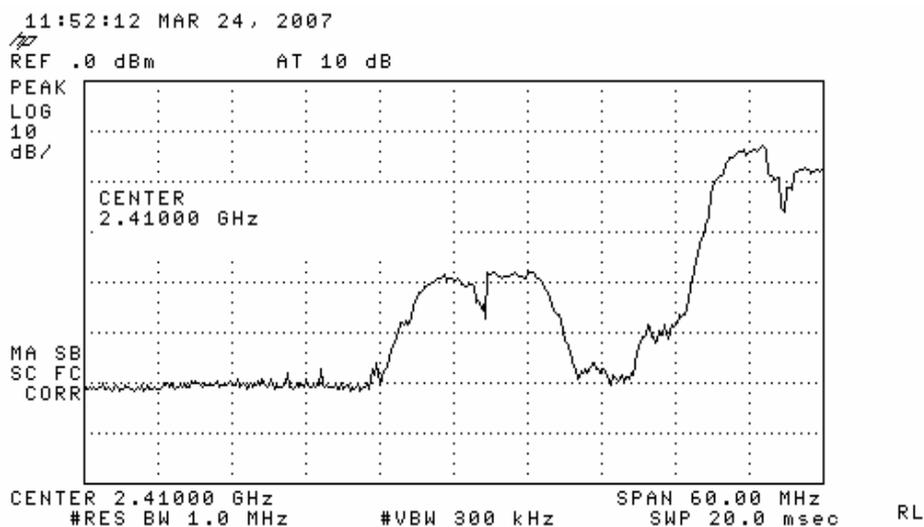


Figura 3.5 Polarización Horizontal

En el gráfico el rango de la señal de interés en el análisis, 2.38 GHz a 2.44 GHz presenta varias portadoras juntas y un valor de densidad espectral de -40 dB.

Valores obtenidos con la antena en Polarización Vertical a 2.41 GHz.

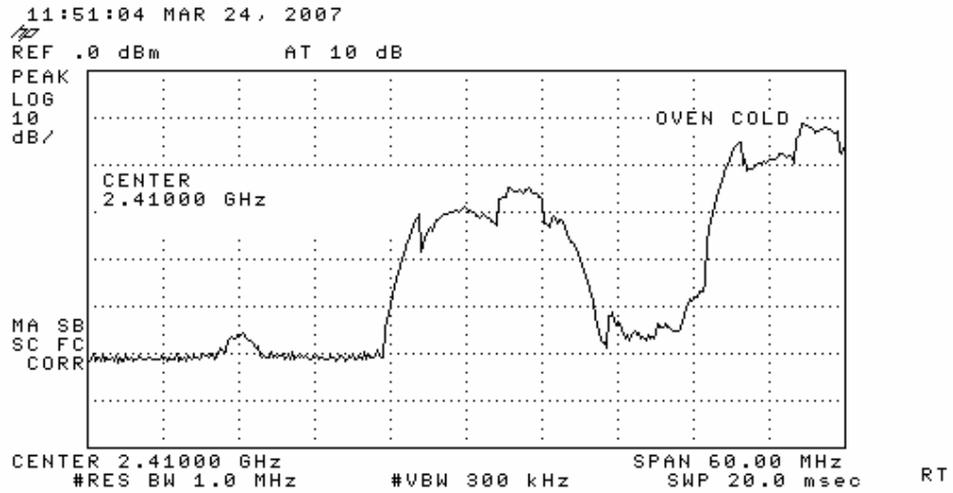


Figura 3.6 Polarización Vertical

En el grafico se observa que en el rango de interés, 2.38 GHz a 2.44, la existencia de varias portadoras y un valor de densidad espectral de -50 dB.

Valores obtenidos con la antena en Polarización Horizontal a 2.437 GHz.

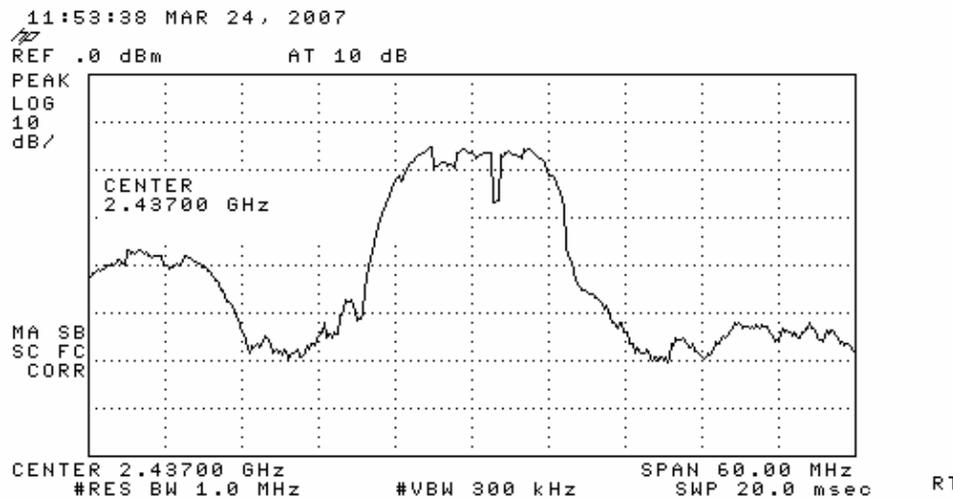


Figura 3.7 Polarización Horizontal

En el grafico, con polarización horizontal, en el rango de 2.407 GHz a 2.467 GHz se observa la presencia varias portadoras y se obtiene una densidad espectral de -63 dB

Valores obtenidos con la antena en Polarización Vertical a 2.437 GHz

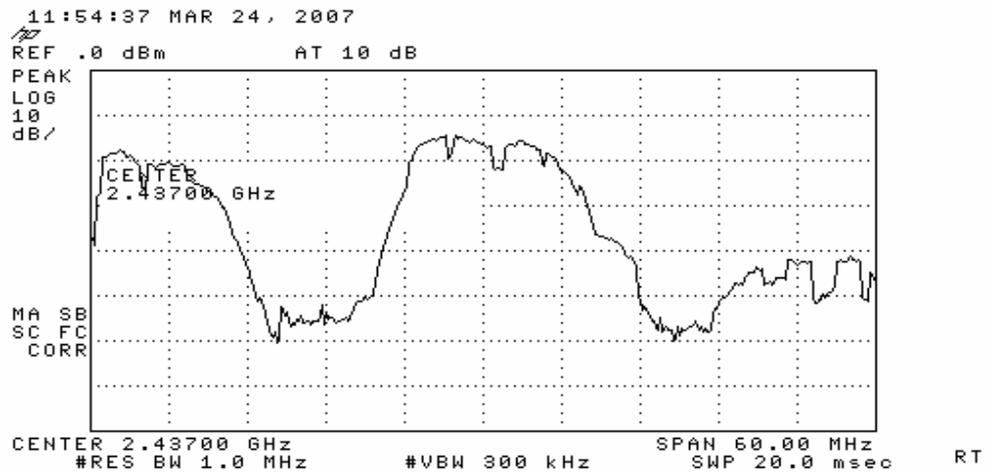


Figura 3.8 Polarización Vertical

En el grafico, con polarización vertical, en el rango de 2.407 GHz a 2.467 GHz se observa la presencia varias portadoras y se obtiene una densidad espectral de -63 dB.

El calculo de propagación radioeléctrica completo, para el Edificio de Administración Central se encuentra descritos en el **anexo 2**

3.2.3 Edificio de la Facultad de Filosofía

Este edificio tiene la mismas características que el edificio de administración, la única variación esta en que en este lugar existen en el 4to piso laboratorios de computadores lo cual haría que la cantidad de usuarios pueda disminuir, para el calculo en general de todo el campus se ha tomado valores similares para obtener resultados cercanos a la realidad existente. Con esta disposición, se puede conseguir conexión también en las gradas de acceso al piso superior e inferior. El espectro en el interior del edificio sera muy semejante al obtenido en Edificio de Administración.

3.2.4 Edificio de la Facultad de Diseño

Este edificio tiene una disposición diferente con respecto a los anteriormente descritos, por esta razón los resultados obtenidos en este lugar serán diferentes ya que no existe la misma cantidad de Access Point que en las otras facultades, lo que hará que el espectro no tenga la misma densidad espectral utilizada.

Los valores tomados del espectro en este sector de la universidad fueron realizados en el exterior del edificio y también nos ayudara con una visión del espectro para la facultad de filosofía.

Valores obtenidos con la antena en Polarización Horizontal a 2.41 GHz.

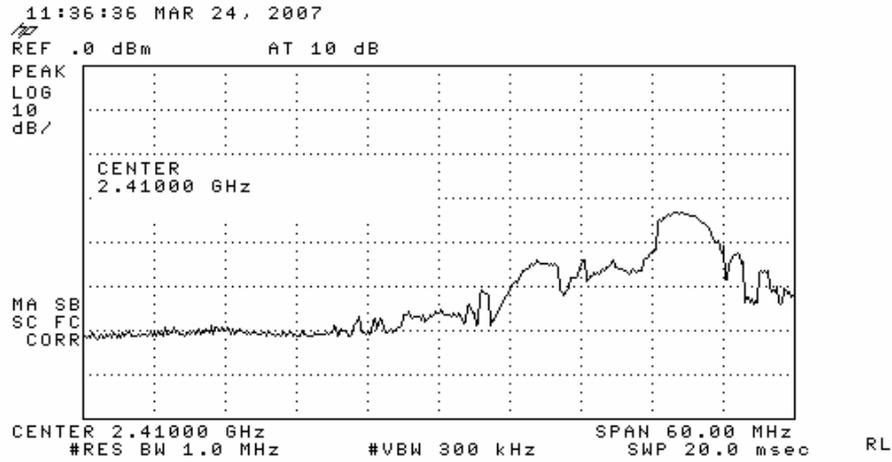


Figura 3.9 Polarización Vertical

En la figura se observa que dentro del rango de interés, 2.38 GHz a 2.44 GHz no existen portadoras y el valor de densidad espectral es -25 dB.

Valores obtenidos con la antena en Polarización Vertical a 2.41 GHz.

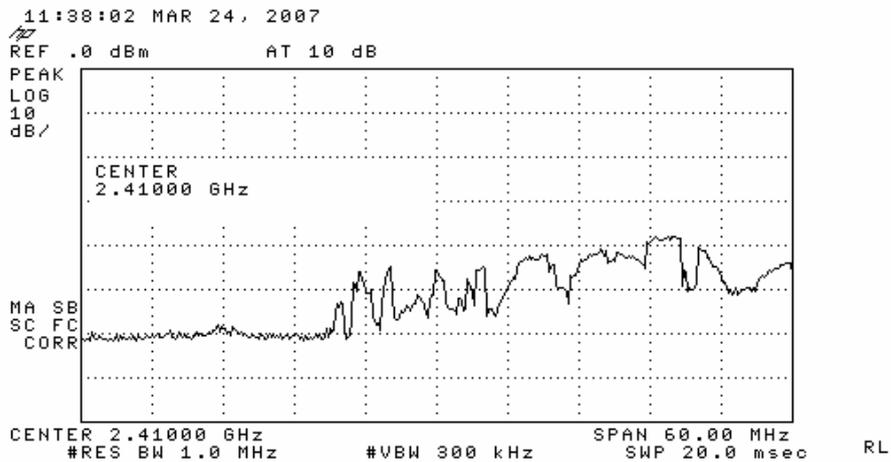


Figura 3.10 Polarización Vertical

En la figura se observa que dentro del rango de interés, 2.38 GHz a 2.44 GHz no existen portadoras y el valor de densidad espectral es -30 dB.

Valores obtenidos con la antena en Polarización Horizontal a 2.437 GHz.

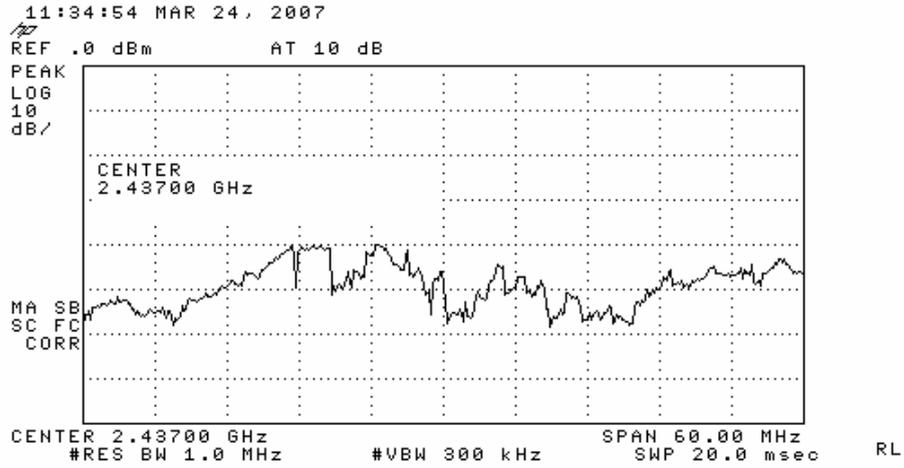


Figura 3.11 Polarización Horizontal

En la figura se observa que dentro del rango de interés, 2.407 GHz a 2.467 GHz no existen portadoras y el valor de campo es -30 dB.

Valores obtenidos con la antena en Polarización Vertical a 2.437 GHz.

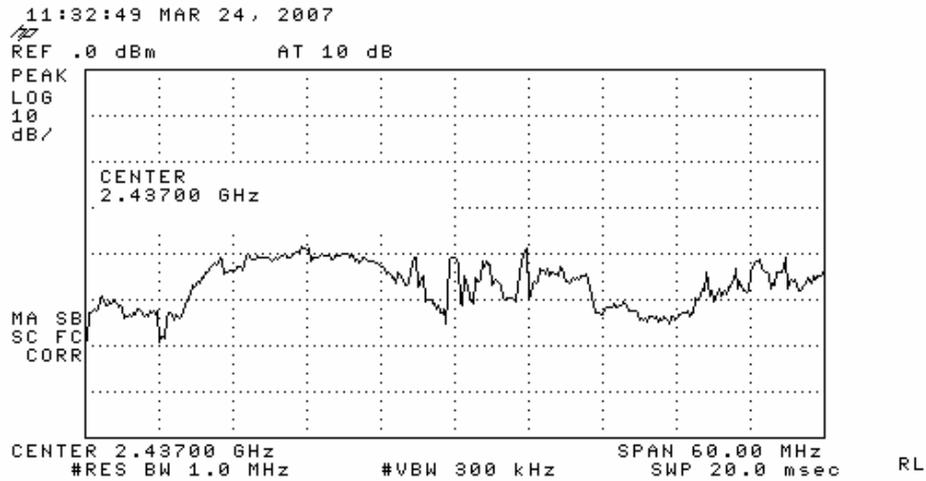


Figura 3.12 Polarización Vertical

En la figura se observa que dentro del rango de interés, 2.407 GHz a 2.467 GHz no existen portadoras y el valor de campo es -40 dB.

3.2.5 Laboratorios de Electrónica

En este lugar se ha tomado un Access Point para los cálculos y diseño, la cantidad de usuarios a servir en este campus es menor ya que en el edificio existen mas laboratorios y no como los otros edificios que existe mas aulas en donde es mayor la cantidad de alumnos.

Los valores tomados del espectro en este sector de la universidad fueron realizados en el exterior del edificio y también nos ayudara con una visión del espectro para la Facultad de Ciencias y Tecnología.

Valores obtenidos con la antena en Polarización Horizontal a 2.41 GHz.

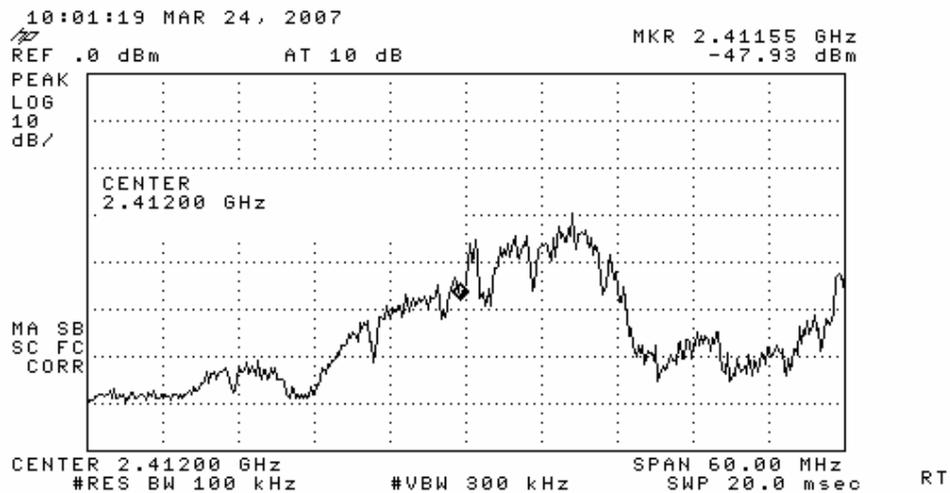


Figura 3.13 Polarización Horizontal

En la figura se observa que dentro del rango de interés, 2.38 GHz a 2.44 GHz existen varias portadoras y el valor de densidad espectral es -45 dB.

Valores obtenidos con la antena en Polarización Vertical a 2.41 GHz.



Figura 3.14 Polarización Vertical

En la figura se observa que dentro del rango de interés, 2.38 GHz a 2.44 GHz existen varias portadoras y el valor de densidad espectral es -45 dB.

Valores obtenidos con la antena en Polarización Horizontal a 2.437 GHz.

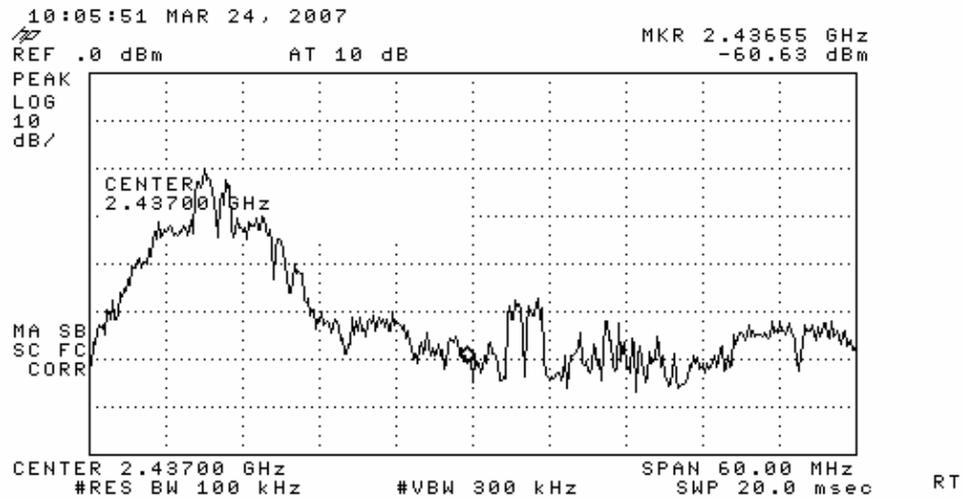


Figura 3.15 Polarización Vertical

En la figura se observa que dentro del rango de interés, 2.407 GHz a 2.467 GHz no existen portadoras y el valor de densidad espectral es -20 dB.

Valores obtenidos con la antena en Polarización Vertical a 2.437 GHz.

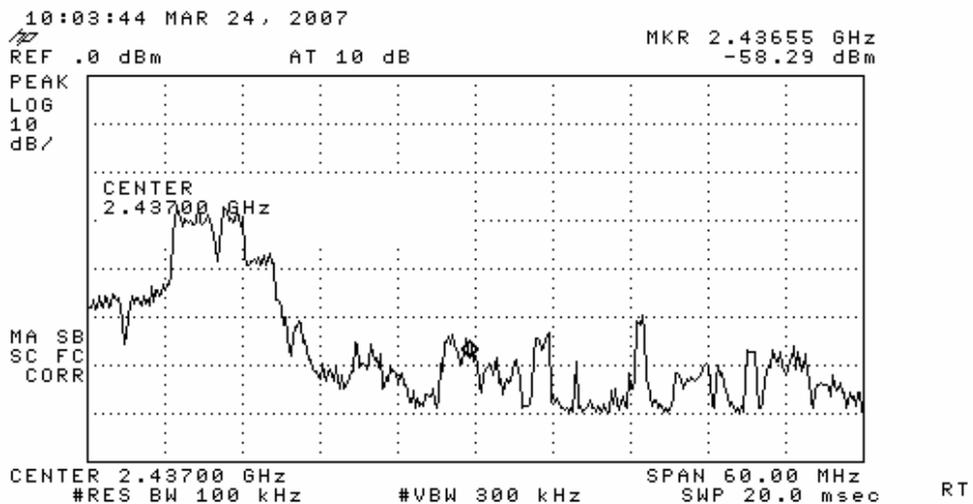


Figura 3.16 Polarización Vertical

En la figura se observa que dentro del rango de interés, 2.407 GHz a 2.467 GHz no existen portadoras y el valor de densidad espectral es -20 dB.

Luego de realizar el Survey de Frecuencias de toda la Universidad del Azuay, podemos observar que el espectro radioeléctrico, en donde se encuentra trabajando la WLAN se encuentra con una ocupación alta, esto es causado no solo por los Access Point existentes en el Campus Universitario, sino además por otros equipos de Radiocomunicaciones que se encuentran trabajando en esta banda que es de uso libre. Los diferentes problemas que causan esta cantidad de señales como ISI, interferencias cocanal y atenuaciones, etc, han sido asumidos al momento de tomar los datos de potencia reales en todos los lugares de la Universidad.

3.3 CALCULOS DEL MODELO

Una vez obtenidos los datos, se deben procesar para obtener la media y la desviación típica. En el caso de las medidas con LOS, la media será la variable n .

Los datos obtenidos de las mediciones con NLOS, se pueden promediar también para corregir (ajustar) las pérdidas por atravesar obstáculos.

A partir de estos datos se calcula el valor de la variable de pérdida de propagación como la media aritmética del resultado de su resolución, según la formula general del modelo:

$$PR(d) = PL(d_0) + 10 \cdot n \cdot \log_{10} \left(\frac{d}{d_0} \right)$$

Donde:

PL (d0) =	pérdida a distancia cercana de referencia
PR (d) =	pérdida a distancia mayor a la referencia
n =	variable de pérdida de trayecto
d =	distancia a la cual se toma la medición PR (d)
d0 =	distancia de referencia a la que se toma PL (d0)

Despejando n :

$$n = \frac{PR(d) - PL(d_0)}{10 \cdot \log_{10} \left(\frac{d}{d_0} \right)}$$

Con las mediciones y utilizando la fórmula se obtienen los valores de n mostrados en el **anexo 2**, para cada uno de los sectores de la Universidad.

Luego de realizado el calculo del valor de n , con estos valores se procede ha calcular la varianza par finalmente calcular la desviación estándar. La fórmula utilizada para determinar la desviación típica es:

$$PL(d) = PL(d_0) + 10n \log(d/d_0) + X_\sigma$$

Donde:

Xs - desviación típica

Como se observa a la fórmula anterior se le suma el valor de Xs, la misma es una variable aleatoria expresada en dB que indica una desviación típica de s dB. En el **anexo 2** se muestran en detalle todos los valores calculados. En la tabla se muestra un resumen de los valores calculados a partir de las mediciones realizadas en los diferentes recintos.

RESUMEN DE CALCULOS

ENTORNO	n MEDIO	DESVIACION	VARIANZA
Biblioteca	1,47703535	4,02101170	16,16853507
Administración P.B.	1,12639296	5,36587131	28,79257487
Administración P1	1,31313623	3,78320642	14,31265078
Administración P2	1,08762859	6,17191058	38,09248021
Administración P3	1,18850047	4,53920925	20,60442060
Administración P4	1,28217694	4,07016493	16,56624254
Filosofía PB	1,30322391	4,51518370	20,38688383
Filosofía P1	1,41879866	3,14987461	9,92171007
Filosofía P2	1,29291479	4,85969592	23,61664444
Filosofía P3	1,54932581	4,06336224	16,51091271
Filosofía P4	1,29641201	5,53038580	30,58516706
Decanato de Investigaciones y Centro de Computo	1,10624441	4,51477478	20,38319135
Edificio de Administración Central	1,10624441	4,51477478	20,38319135
Facultad de Ciencias y Tecnología.	1,13381687	5,36221199	28,75331738
Facultad de Diseño	1,01604127	5,83238098	34,01666789
Laboratorio de Electronica	1,45951980	3,60231141	12,97664749

Tabla 3.3 Resumen de Cálculos

Con los valores de la variable de pérdida de trayecto y la desviación típica establecidos, se procede a realizar un cálculo correspondiente al valor de P(R), ya en función del valor de PL (d0) calculado y con el nuevo valor de n considerado en el modelo. Para determinar PL (d0) utilizamos la fórmula:

$$P_r(d) = \frac{P_t G_t G_y \lambda^2}{(4\pi)^2 d^2 L}$$

Donde:

- Pr (d) = potencia recibida; la cual es función de la separación T-R (transmisor-receptor)
- Pt = potencia transmitida
- Gt = ganancia de antena transmisora
- Gr = ganancia de la antena receptora
- ? = longitud de onda en metros
- d = la distancia de separación de T-R en metros
- L = pérdidas del sistema no achacables a la propagación
- Para determinar la ganancia de la antena se puede utilizar la fórmula:

$$G = \frac{4\pi A_e}{\lambda^2}$$

Para el presente diseño consideramos que la ganancia de antena está normalmente dada en decibelios isotrópicos [dBi]. Esta es la ganancia de energía en comparación con una antena isotrópica. Algunas antenas tienen su ganancia expresada en [dBd], es la ganancia comparada con una antena dipolo. En este caso se tiene que sumar 2.14 para obtener la ganancia correspondiente en [dBi]. Cuanta más ganancia tenga la antena mayor es la directiva es decir la energía enviada en una dirección preferida. Las antenas que vienen en los equipos de WLAN generalmente no tienen mucha ganancia, por lo que se asume un valor de 2.14 dBi. La ganancia de antena es la misma para recibir y transmitir.

Con las consideraciones anteriores se establece el modelo como:

$$P(R) = 53 - 20,37 \cdot \log(d)$$

La parametrización de variable X_s se ajusta al valor de la desviación típica de la serie obtenida. No obstante, se deja a consideración del usuario su ajuste ya que puede modelar efectos no previstos en el trayecto como obstáculos humanos, interferencias silenciosas, etc.

La varianza S^2 , se define como la media de las diferencias cuadráticas de n puntuaciones con respecto a su media aritmética,

$$S^2 = \frac{1}{n} \sum_{i=1}^n x_i^2 - \bar{x}^2$$

Para que la medida de dispersión sea de la misma dimensionalidad que las observaciones, bastará con tomar su raíz cuadrada. Por ello se define la desviación típica S , como:

$$S = \sqrt{S^2}$$

Con estos datos, el modelo de propagación directa que se va a utilizar para calcular la pérdida de trayecto en el espacio libre será:

$$P(R) = 53 - 20,37 \log(d) + \text{Aleatorio}$$

La medida aleatoria nos permite simular variaciones de señal causadas por el entorno radioeléctrico. Aunque la señal de cobertura sea aleatoria, nos da una indicación de las variaciones de señal que se producen en las zonas donde χ^2 es significativa respecto al resto de la señal.

3.4 Conclusiones

- ♦ La variable de pérdida de trayecto como ya se mencionó durante el desarrollo depende del tipo de entorno. En el presente proyecto se ha generalizado esta variable para poder utilizarla en un entorno como lo es el de la Universidad del Azuay. Para otros entornos se tienen valores de n típicos como los mostrados en la tabla.

Entorno	n
Edificios (condiciones de visión directa)	1.6 a 2
Edificios (sin visión directa)	2 a 4
Edificios (sin visión directa, separación de uno a tres pisos)	4 a 6

En la Universidad del Azuay se determinan valores de n cuyo valor medio es:

n medio	=	1,26725541
----------------	---	-------------------

Este valor se presenta debido a que los Access Point son considerados en áreas pequeñas, en la mayoría de casos aulas en la que la cobertura de los mismos no sobrepasa los 10m. Para cada entorno se determina un n medio y en función de este se generalizan las pérdidas en el trayecto $P(R)$.

- ♦ Luego de realizado el análisis de la distribución de Access Point se considera el aumentar la cantidad de Access Point en algunos sectores de la universidad. De esta forma se establecen valores de campo óptimos (valores que se desean recibir) para estos lugares y se podrá tener una mejor área de cobertura. Para el cálculo de propagación se considera valores de la variable de pérdida del trayecto dentro del rango de la ya generalizada anteriormente, de igual forma se consideran las pérdidas en el trayecto. Para mirar la propagación referirse al capítulo IV.

CAPITULO IV HERRAMIENTAS DE SIMULACIÓN DE PROPAGACIÓN

4.1 Evaluación de Herramientas

Dentro del análisis de propagación radioeléctrica existen en la actualidad algunas herramientas que permiten observar de manera muy exacta la cobertura de los Access Point que se puedan ubicar en una determinada área estos paquete tienen un costo de alrededor de 10.000 dólares. A continuación citamos algunas:

Xirrus LanPlanner, <http://www.bluesocket.com/products/wireless.html> utiliza formatos dwg el entorno es muy parecido a Autocad. Los valores de propagación se deben ingresar al programa para que este pueda calcular esto se lo puede realizar por cada piso del edificio. El demo solo se puede utilizar con el ejemplo que tiene. Es utilizado en varias universidades para el diseño de propagación de la red wireless

Ekahau site Survey (<http://www.ekahau.com/?id=4600>), realizado en Java se importa un grafico con la planta del edificio y se coloca las paredes, ventanas con las herramientas del programa, este automáticamente regulara la imagen de propagación con los obstáculos que tiene que atravesar esta limitado el tiempo de captura de los Access Point

Isite <http://www.MeritechSolutions.com> igual que el anterior la versión demo solo dura 15 días

rps <http://www.radioplan.com> utiliza cost 231 como modelo de propagación la versión de evaluación esta limitada a 750 polígonos el resto de opciones es completa se pueden adicionar mas modelos de propagación mediante plugin realizados en matlab

4.2 Radiowave Propagation Simulator (RPS)

Luego de realizar un análisis de los software y sus utilidades se ha decidido ocupar el **RPS Radioplan** por ventajas que se han encontrado en este simulador como:

La capacidad que el software tiene de poder encontrar las áreas de cobertura de cada access point con la incorporación de un plugins que se ha desarrollado utilizando el modelo de propagación “*Log-Normal Shadowing Path Loss Model*” y además utilizando el valor de la perdida generalizada por los obstáculos que se tiene en el trayecto y que se calculo en el capítulo III.

Otra ventaja es la factibilidad de poder introducir un plano con medidas exactas y que tenga hasta 750 poligonos dibujados en 3D y que tenga el formato *.dwg, esto permite que los dibujos puedan ser realizados en diferentes software como el microestación, Autocad, Inventor. Para la simulación se ha realizado los planos de la Universidad en 3D, para observar de mejor manera los obstáculos y la propagación en cada uno de los lugares donde se encuentra un Access Point en la Universidad del Azuay.

Los datos que han sido utilizados para todas las simulaciones son los siguientes:

Antena:

Tipo: Isotropic Source
 Ganancia: 2,14 dB
 Polarización: Vertical

Transmisor:

Potencia: 17.92 dBm
 Frecuencia: 2,41 Ghz
 Tipo: Isotropic Source
 Posición: Dependerá de la ubicación dentro de cada plano.

Receptor:

Sensibilidad: -105dB

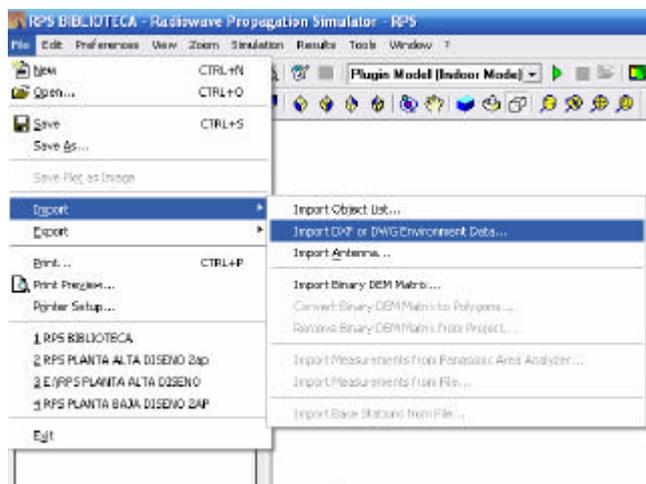
Materiales:

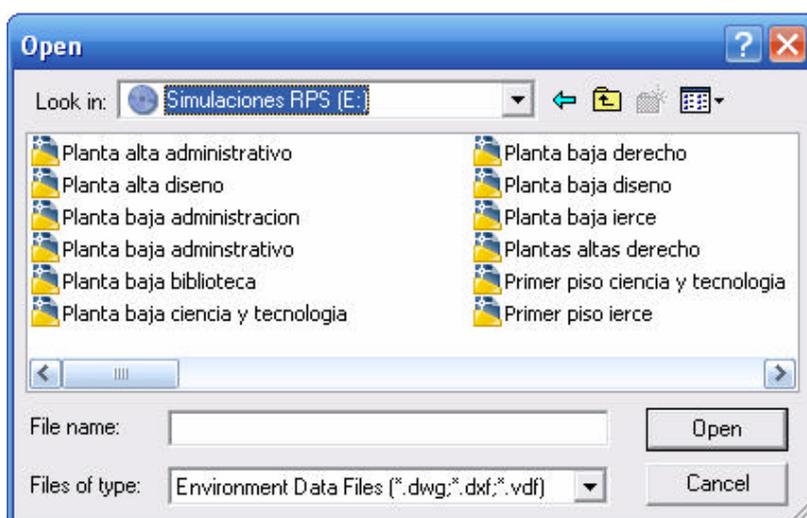
Concreto: 40cm
 Paredes: 20 cm
 Vidrio: 2cm
 Madera: 5cm

4.2.1 Descripción del Uso del Programa de Simulación



1. Introducir el plano del lugar donde se va a realizar la simulación (plano realizado en 3D con la cantidad de poligonos necesarios para una mejor simulación), además realizar la ubicación de los Access Point dentro del plano.

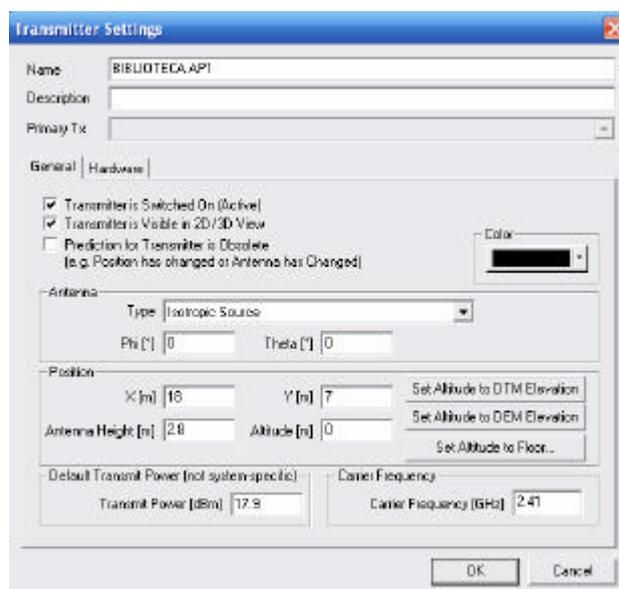




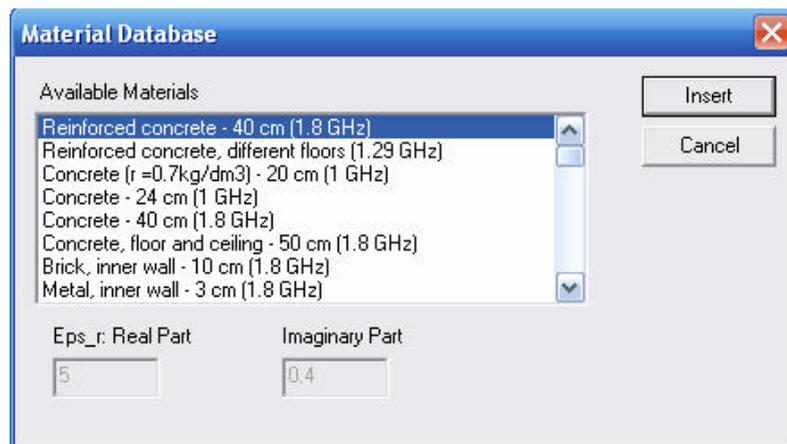
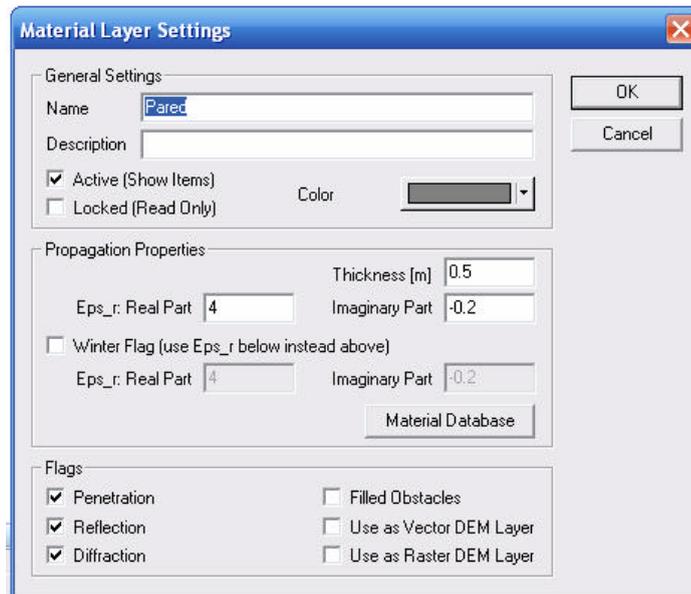
2. Escoger tipo de antena, ganancia y polarización.



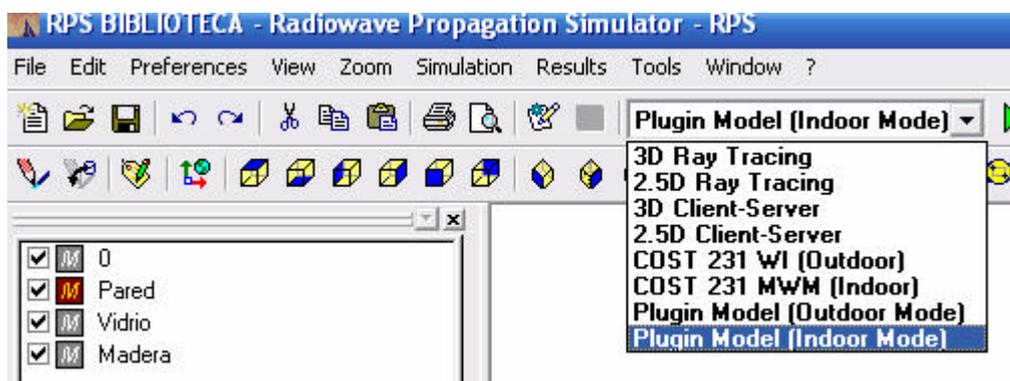
3. Cargar los datos del transmisor, tipos de antena y frecuencia en la que se realiza la simulación.



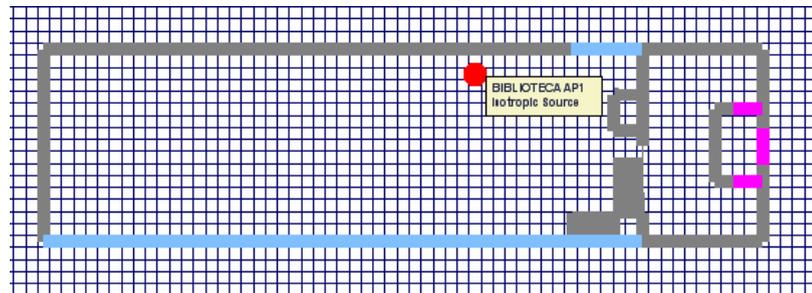
4. Cargar datos de espesor de cada uno de los materiales de que esta compuesto las paredes, vidrios, puertas, etc. del lugar.



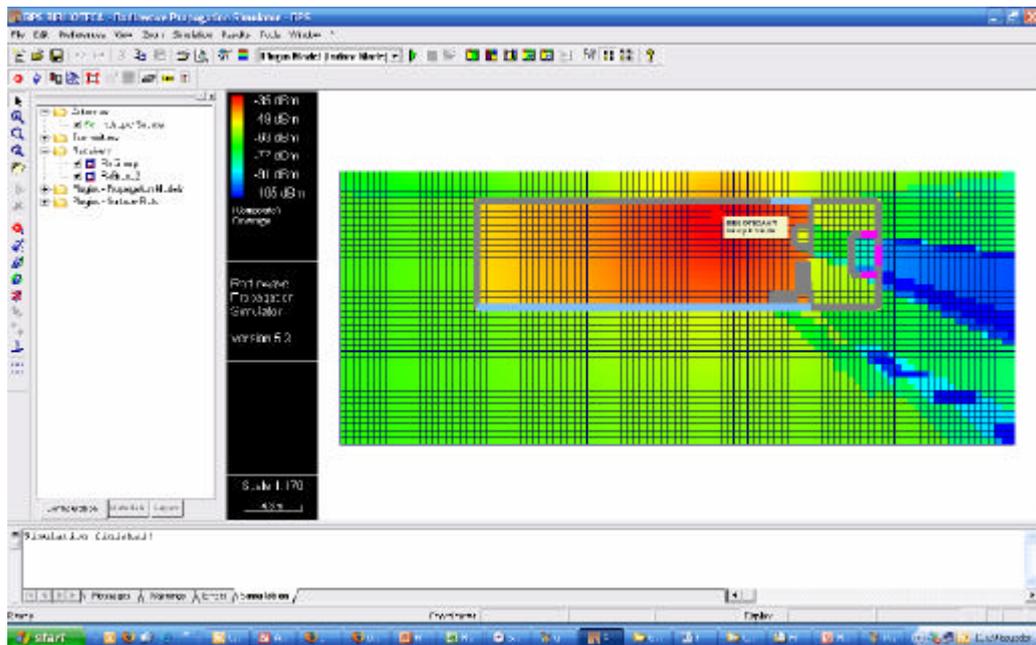
5. Escoger el tipo de modelo que se utilizara para la simulación en nuestro caso ‘*Log-Normal Shadowing Path Loss Model*’, este será realizado con el plugins que se desarrollo para obtener las coberturas de los Access Point.



- Dibujar el área de análisis en el plano para poder visualizar la propagación.

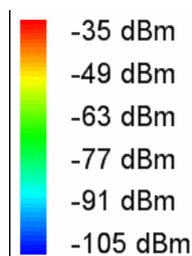


- Inicializar la simulación.
- Verificar el campo existente para cada uno de los Access Point.

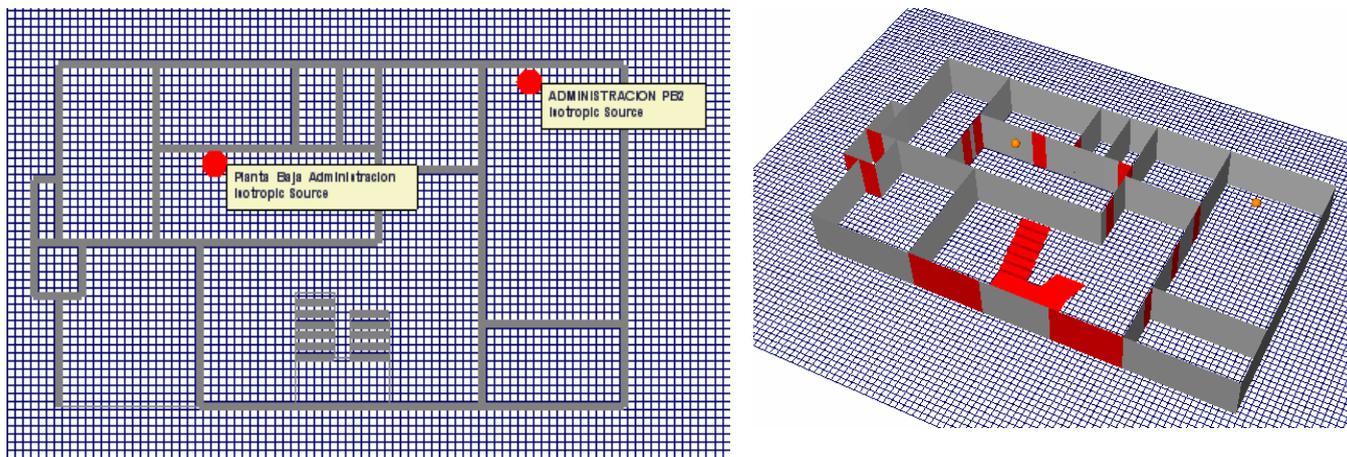


Luego de realizar todo este procedimiento se obtienen los siguientes resultados , los cuales nos mostraran las coberturas para cada una de las áreas propuestas para dar acceso a los usuarios.

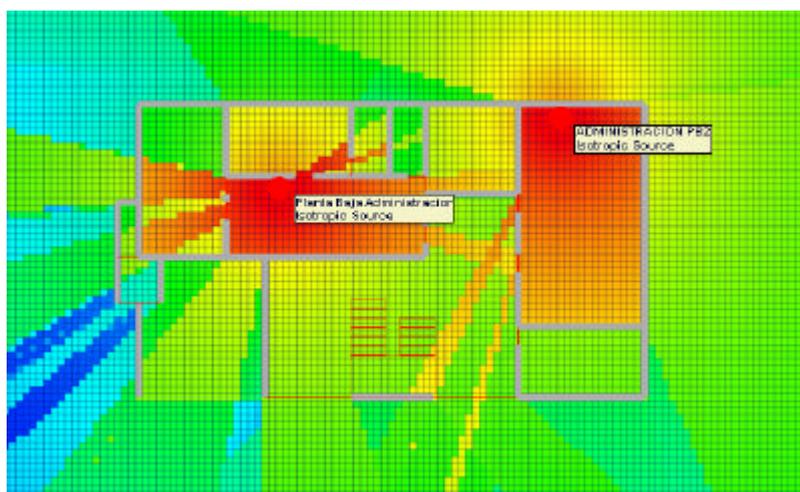
Resultados de áreas de cobertura y Propagación de los Access Point existentes en la Universidad del Azuay. El valor de campo es de acuerdo a los colores y cada uno significa un valor como se ve en la siguiente grafica.



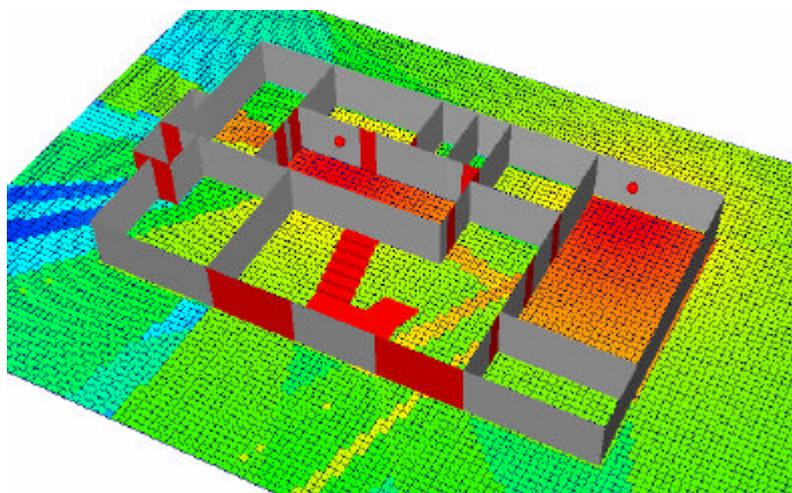
4.3 SIMULACION DE ADMINISTRACION PLANTA BAJA



Ubicación de Access Point y Plano de la Planta Baja

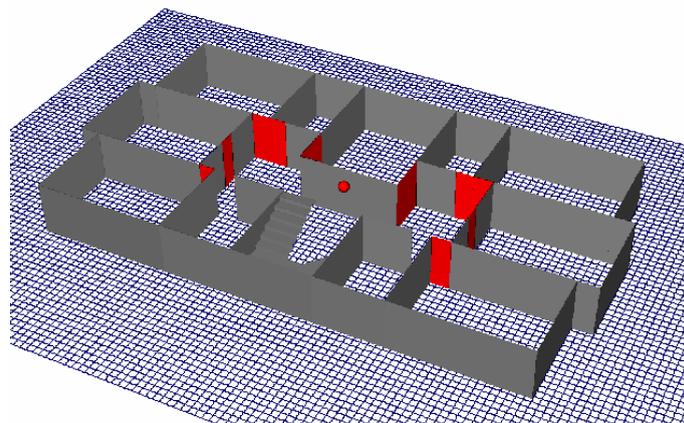
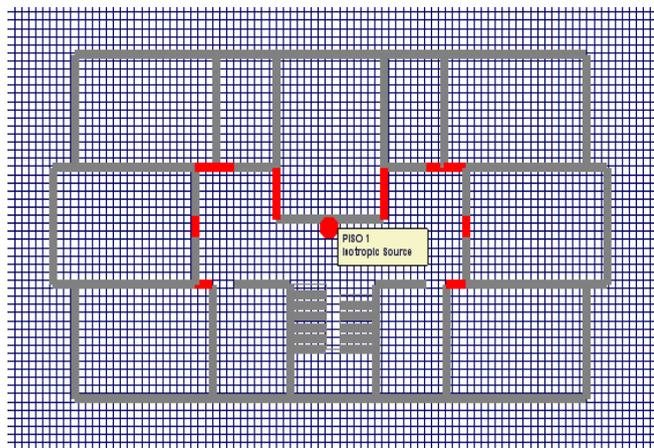


Propagación en 2D en Administración Planta Baja

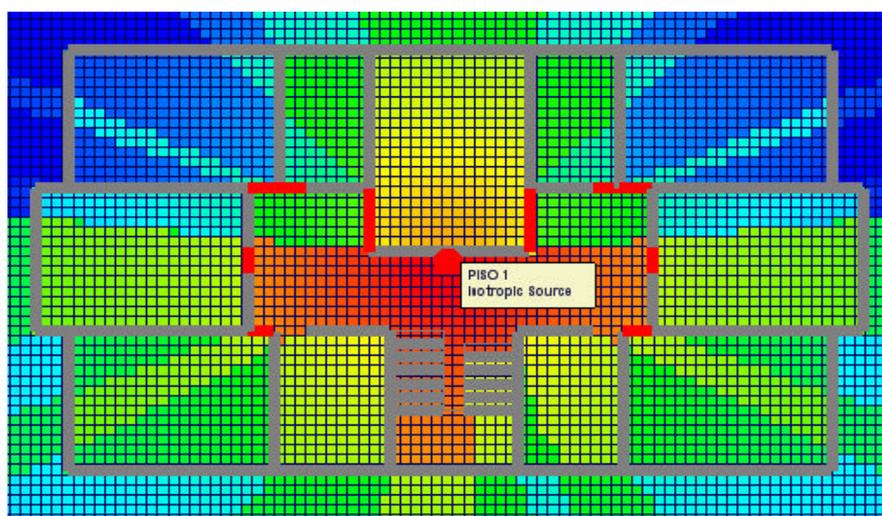


Propagación en 3D en Administración Planta Baja

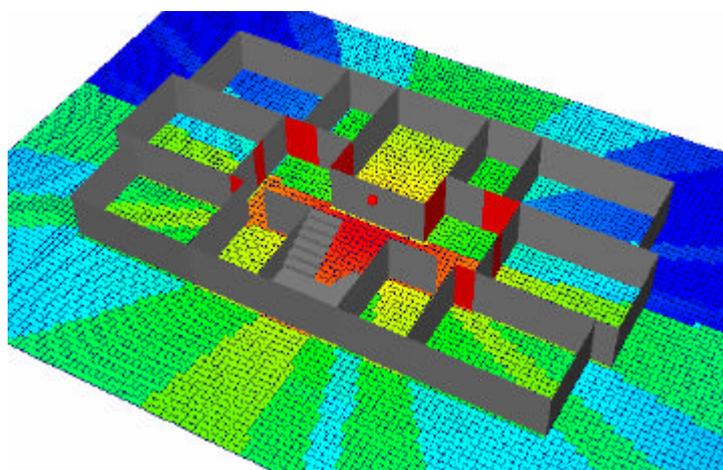
4.4 SIMULACIÓN DE ADMINISTRACION PISO 1



Ubicación de Access Point y Plano PISO 1

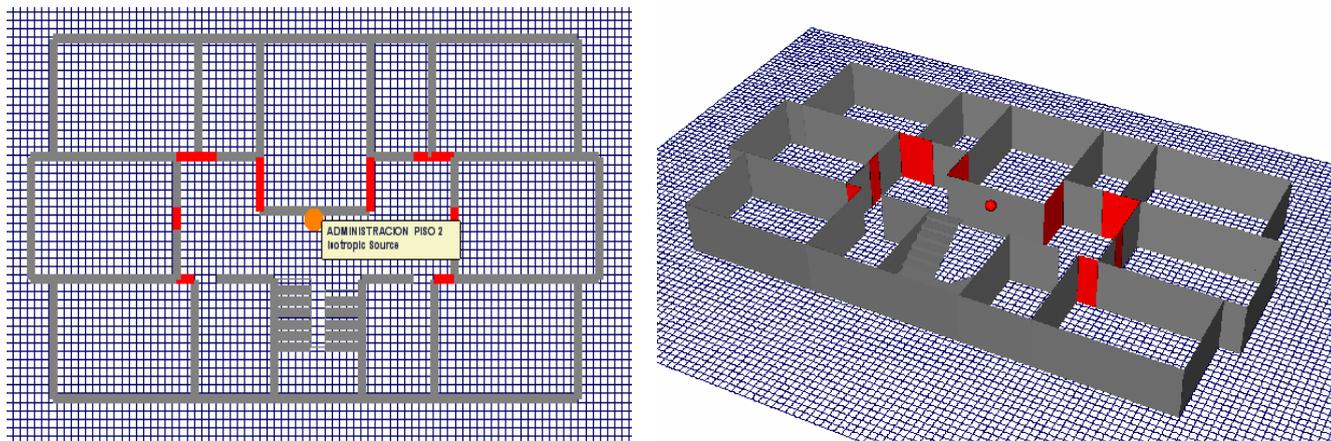


Propagacion en 2D en Administración PISO 1

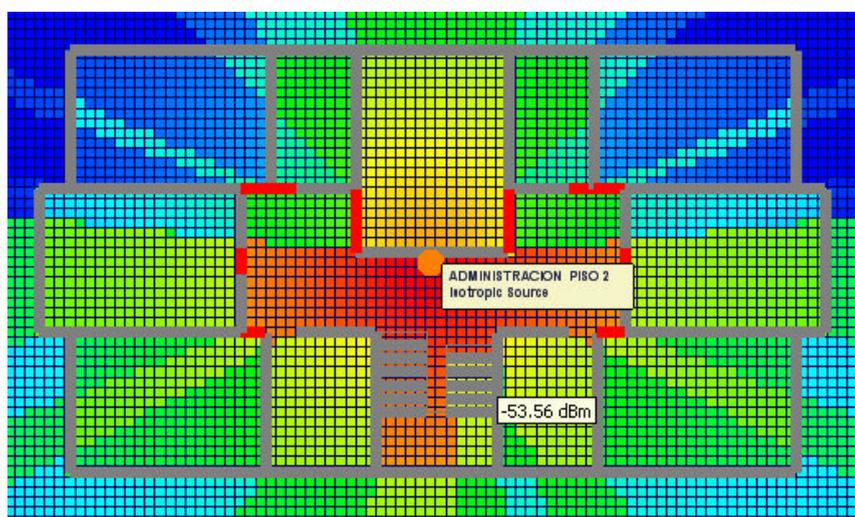


Propagacion en 3D en Administración PISO 1

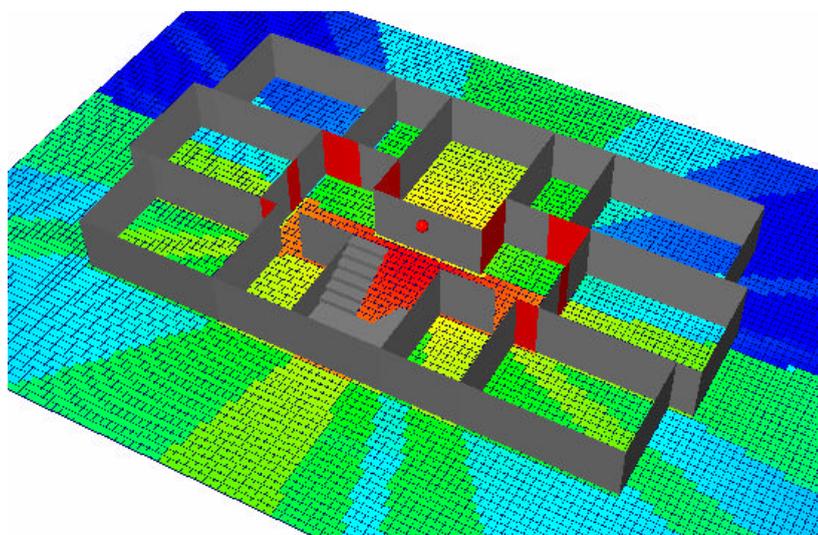
4.5 SIMULACIÓN DE ADMINISTRACION PISO 2



Ubicación de Access Point y Plano de la PISO 2

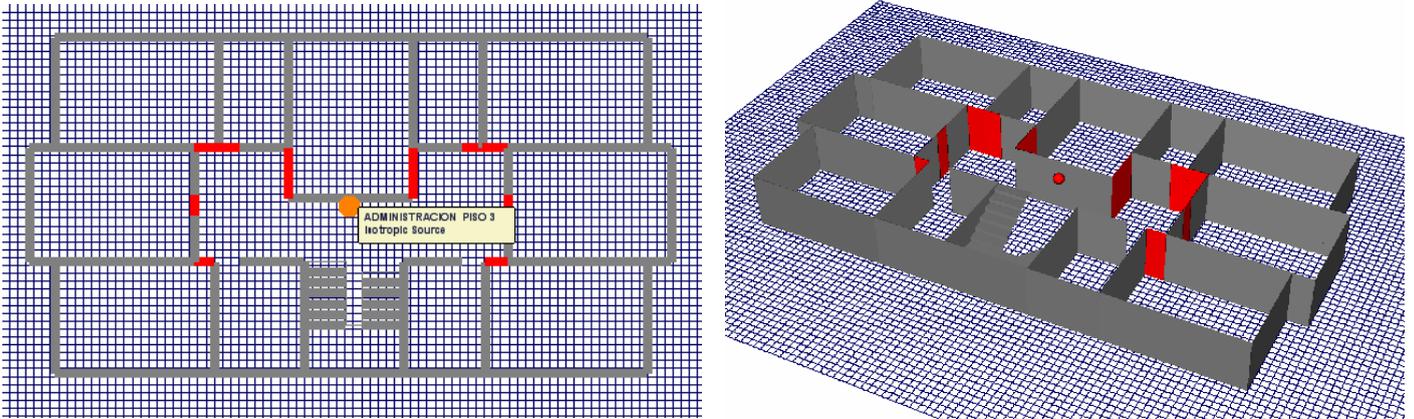


Propagacion en 2D en Administración PISO 2

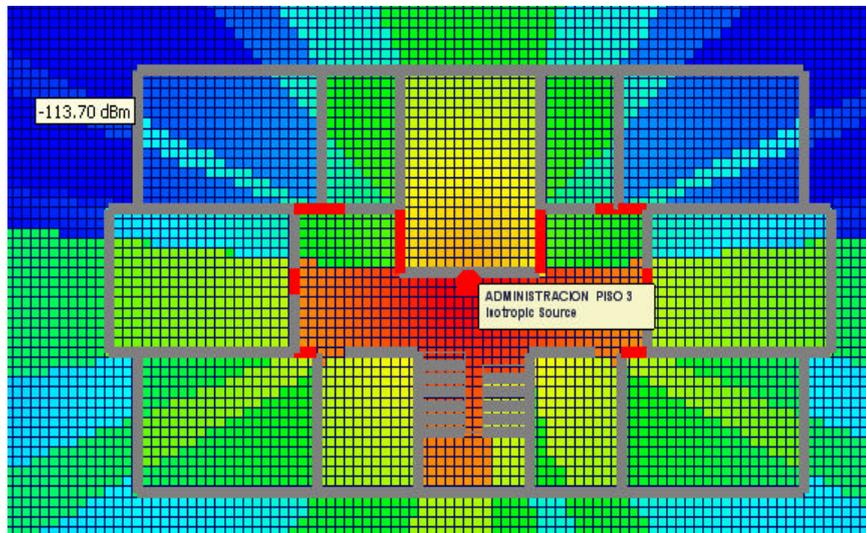


Propagacion en 3D en Administración PISO 2

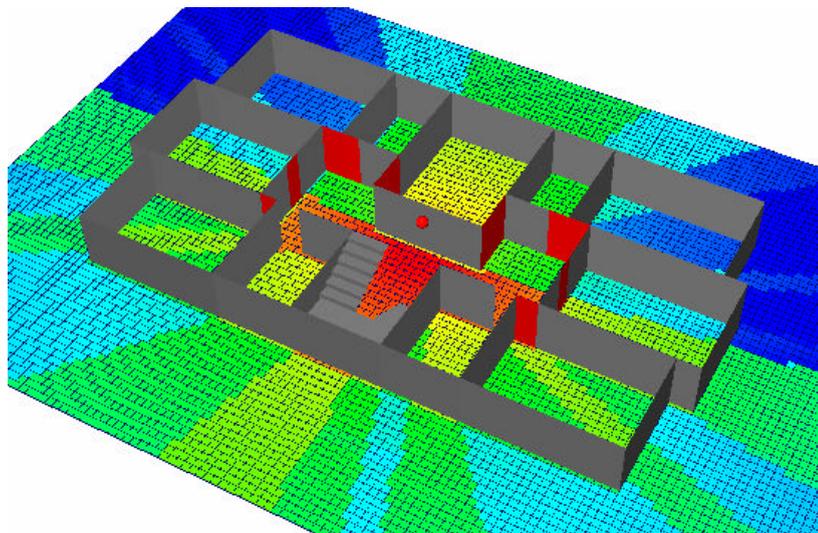
4.6 SIMULACIÓN DE ADMINISTRACION PISO 3



Ubicación de Access Point y Plano de la PISO 3

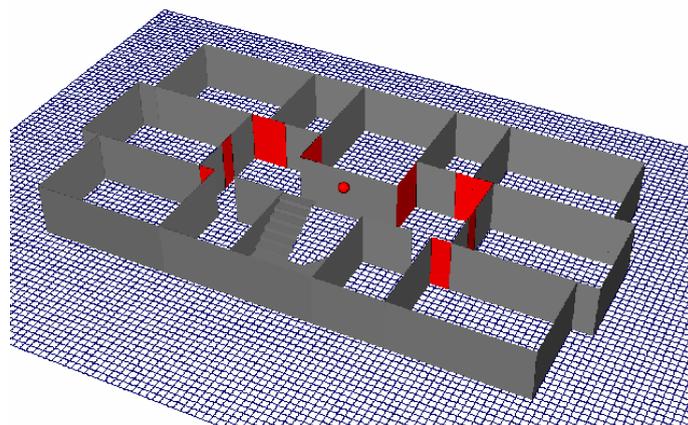
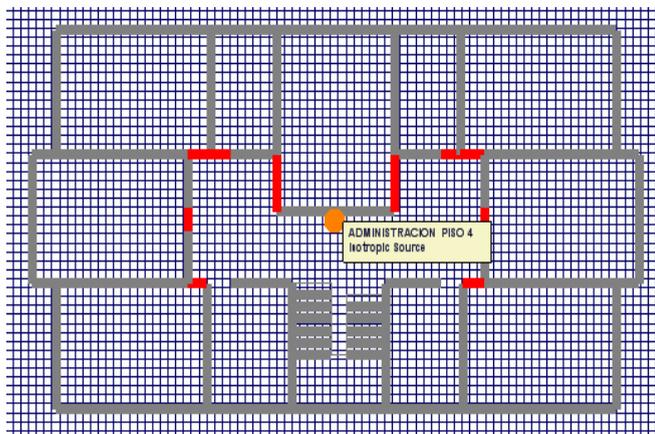


Propagacion en 2D en Administración PISO 3

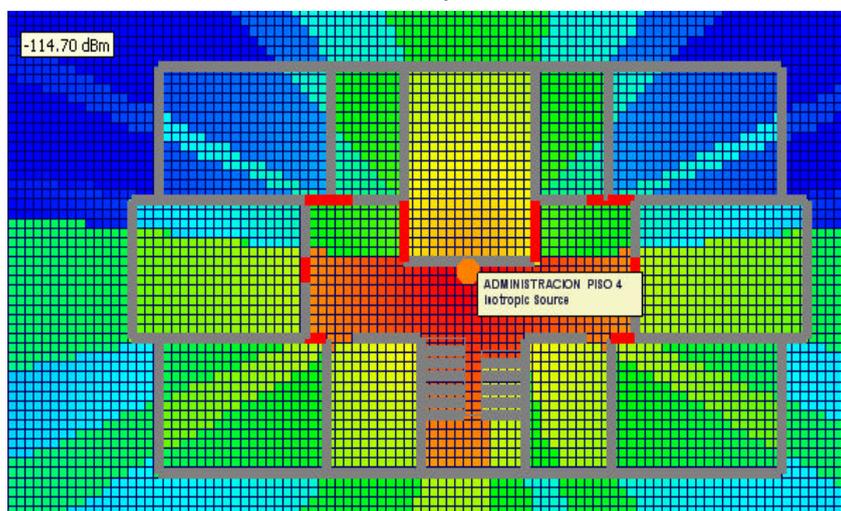


Propagacion en 3D en Administración PISO 3

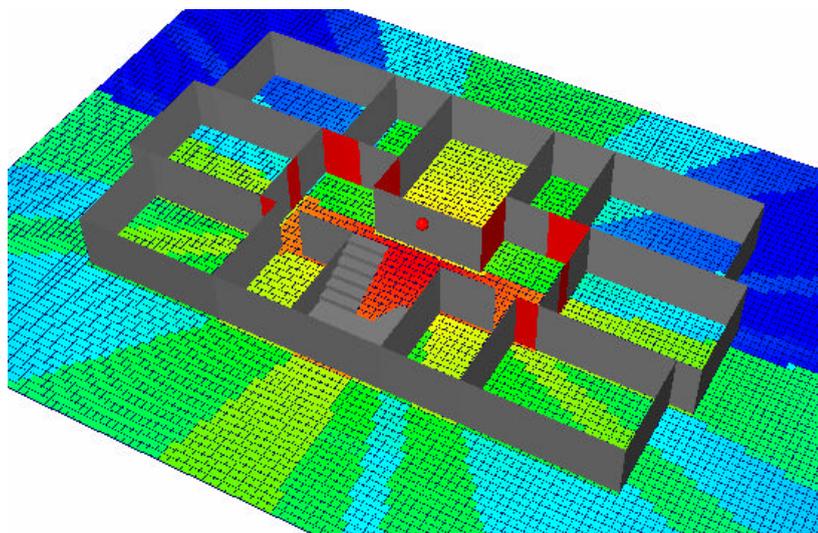
4.7 SIMULACIÓN DE ADMINISTRACION PISO 4



Ubicación de Access Point y Plano de la PISO 4

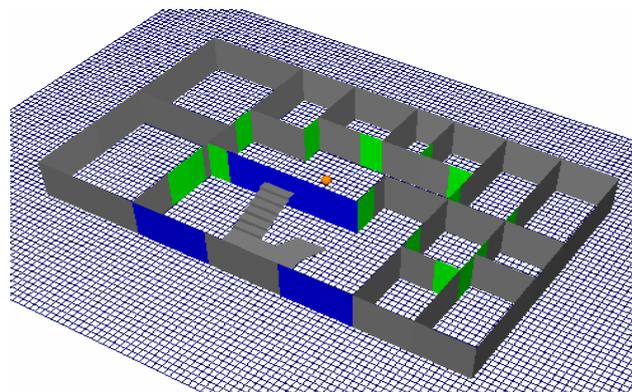
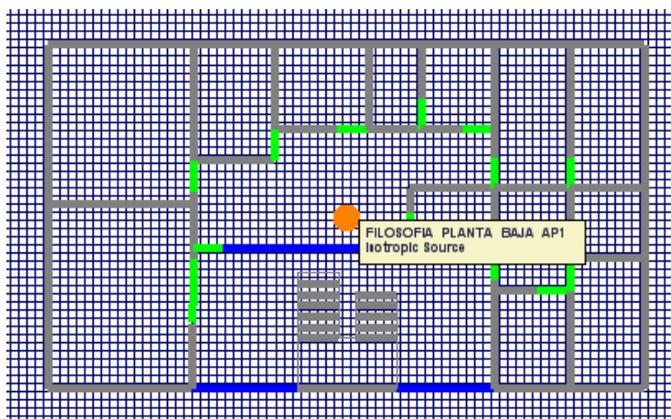


Propagación en 2D en Administración PISO 4



Propagación en 3D en Administración PISO 4

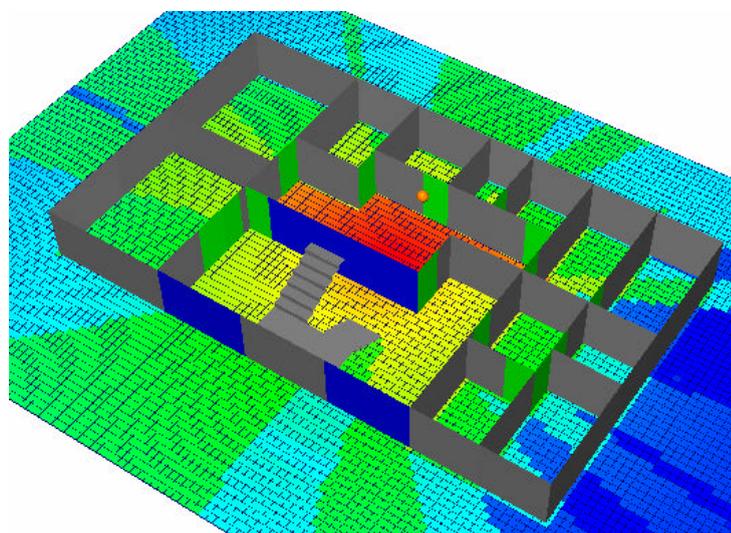
4.8 SIMULACIÓN DE FILOSOFIA PLANTA BAJA



Ubicación de Access Point y Plano de la PLANTA BAJA

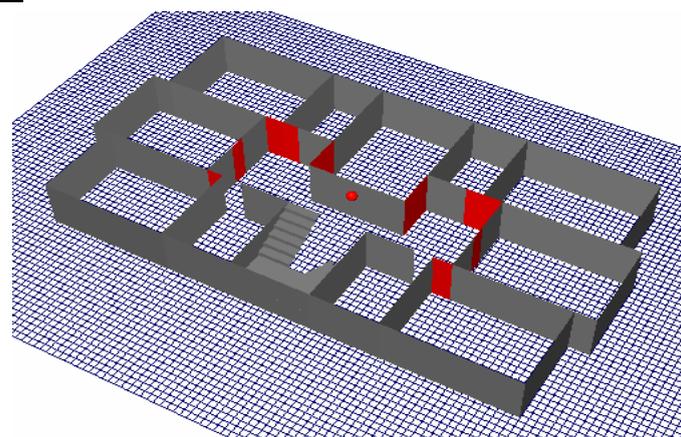
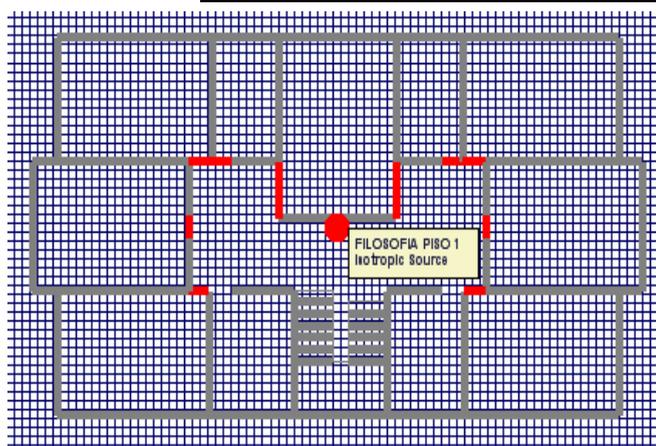


Propagación en 2D en Filosofía PLANTA BAJA

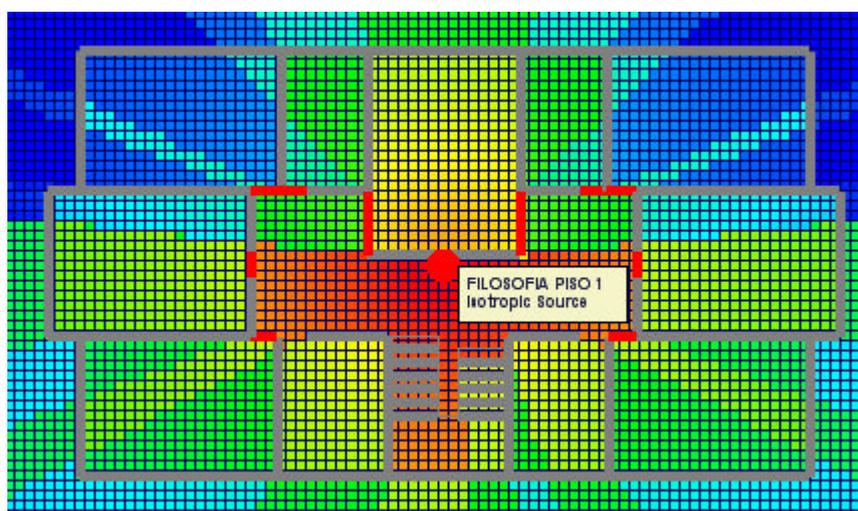


Propagación en 3D en Filosofía PLANTA BAJA

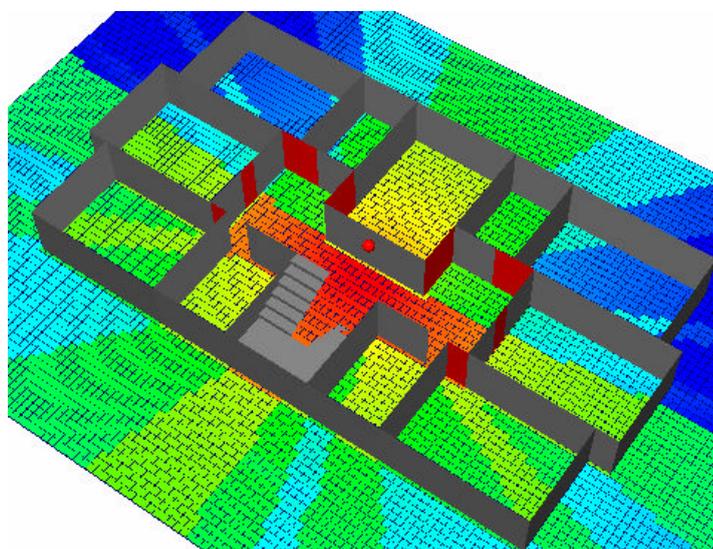
4.9 SIMULACIÓN DE FILOSOFIA PISO 1



Ubicación de Access Point y Plano del PISO 1

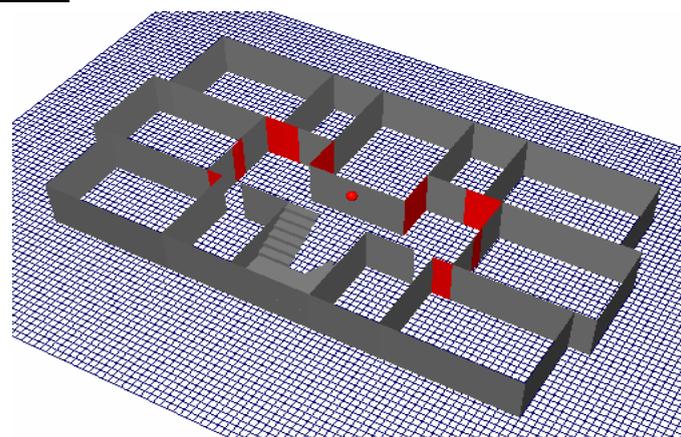
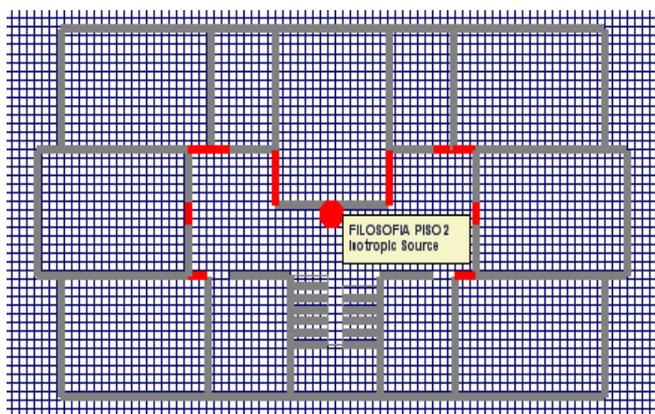


Propagación en 2D en Filosofía PISO 1

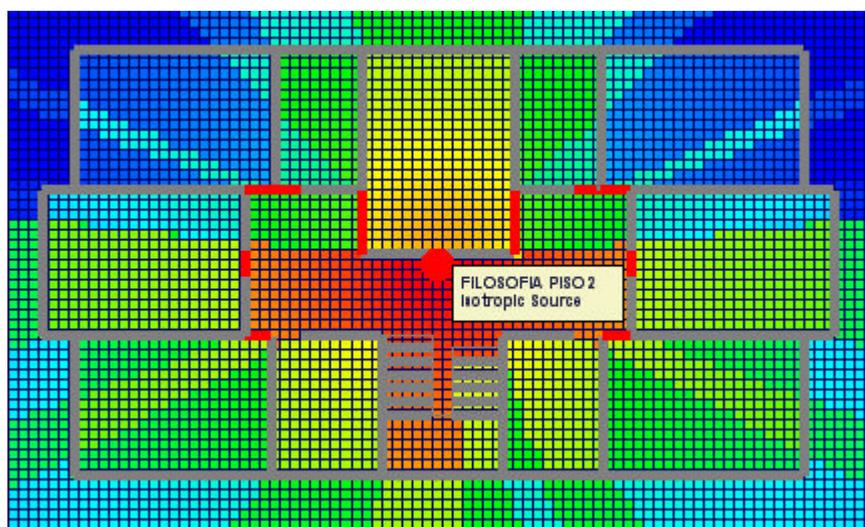


Propagación en 3D en Filosofía PISO 1

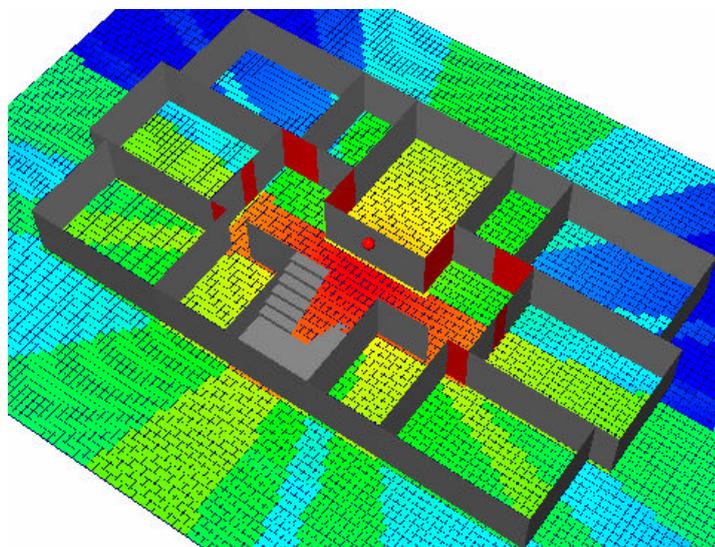
4.10 SIMULACIÓN DE FILOSOFIA PISO 2



Ubicación de Access Point y Plano del PISO 2

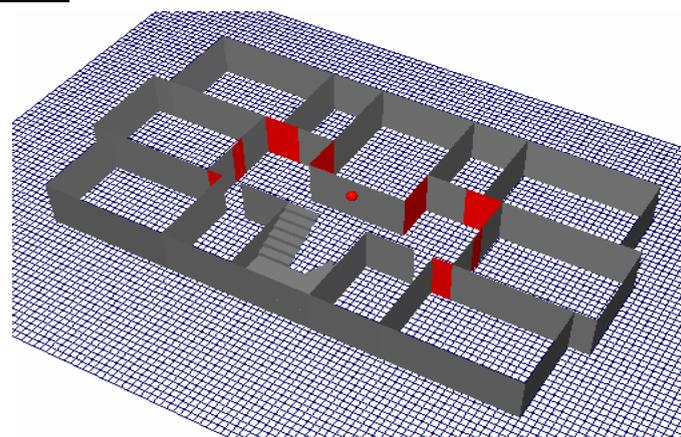
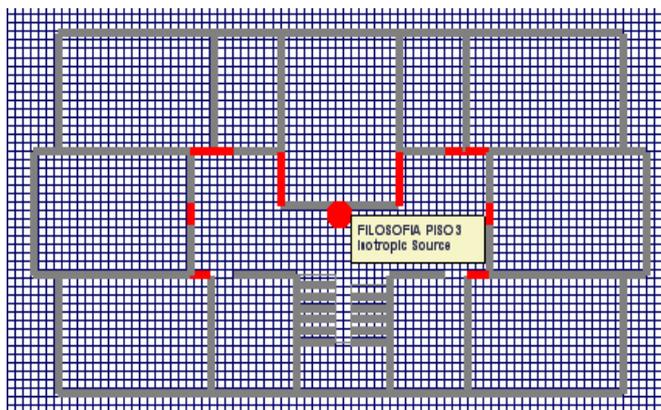


Propagación en 2D en Filosofía PISO 2

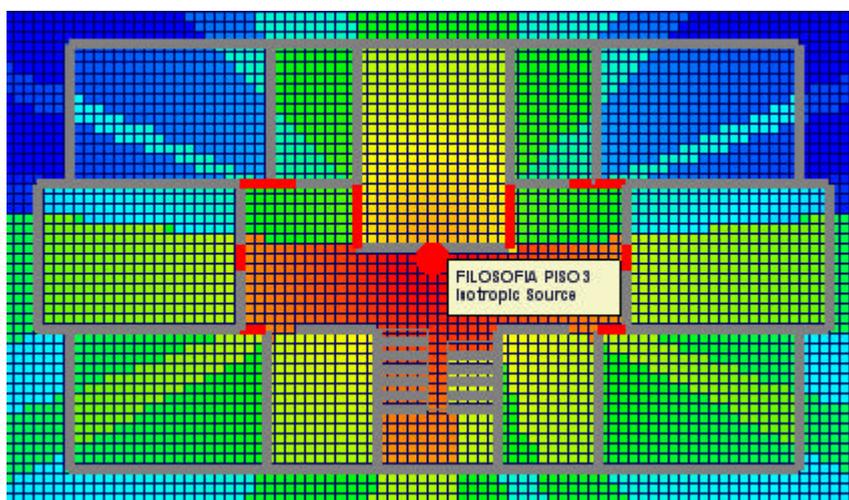


Propagación en 3D en Filosofía PISO 2

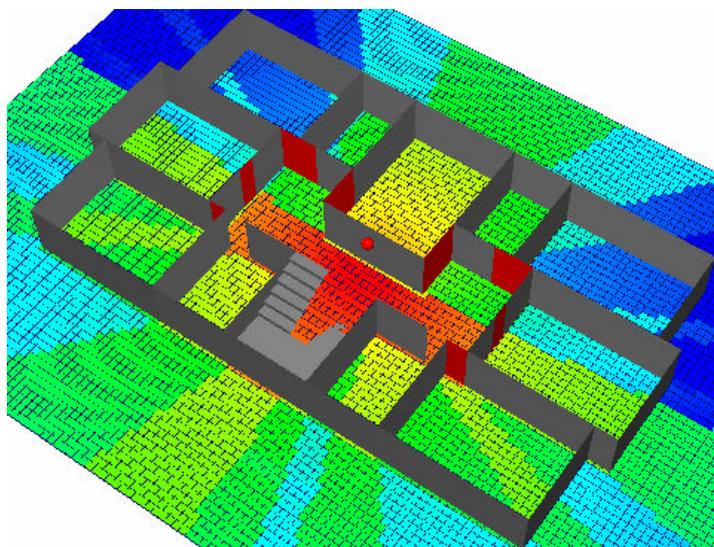
4.11 SIMULACIÓN DE FILOSOFIA PISO 3



Ubicación de Access Point y Plano del PISO 3

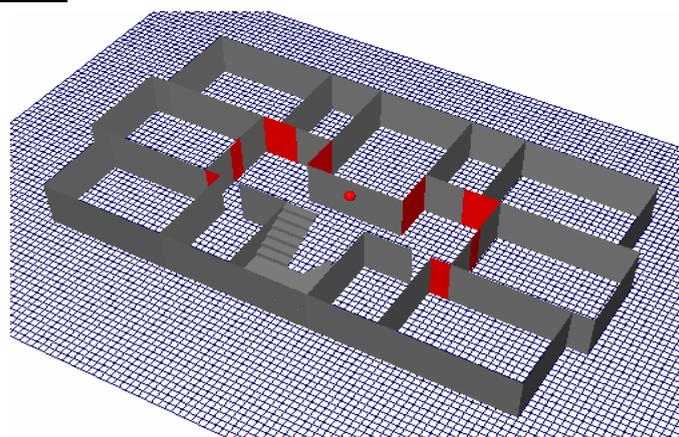
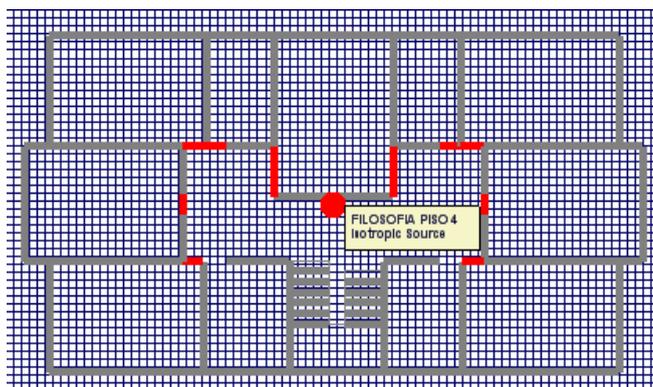


Propagación en 2D en Filosofía PISO 3

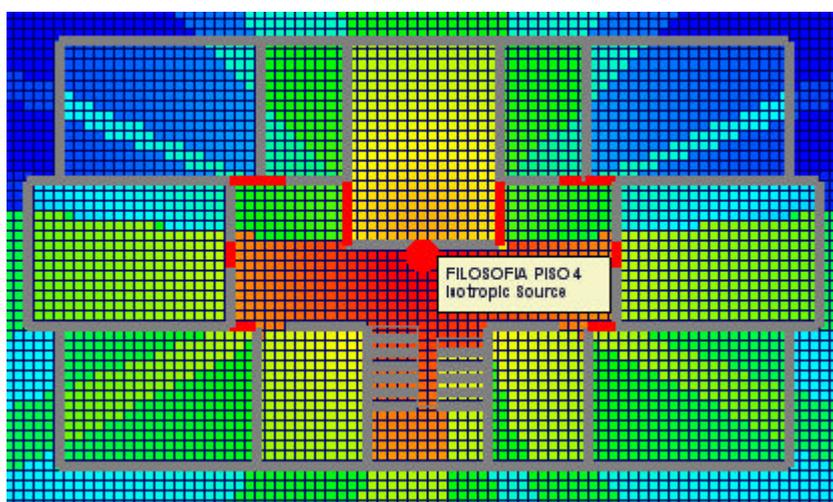


Propagación en 3D en Filosofía PISO 3

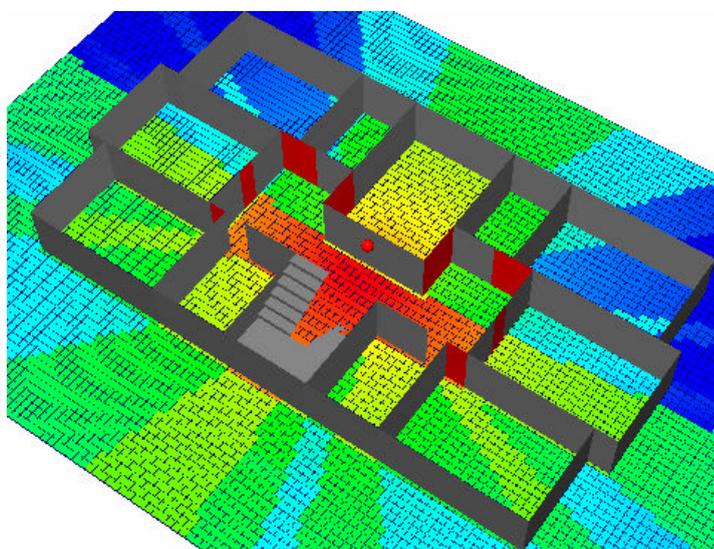
4.12 SIMULACIÓN DE FILOSOFIA PISO 4



Ubicación de Access Point y Plano del PISO 4

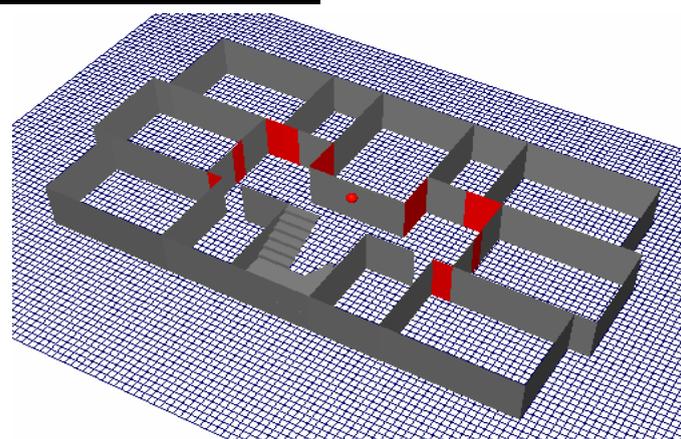
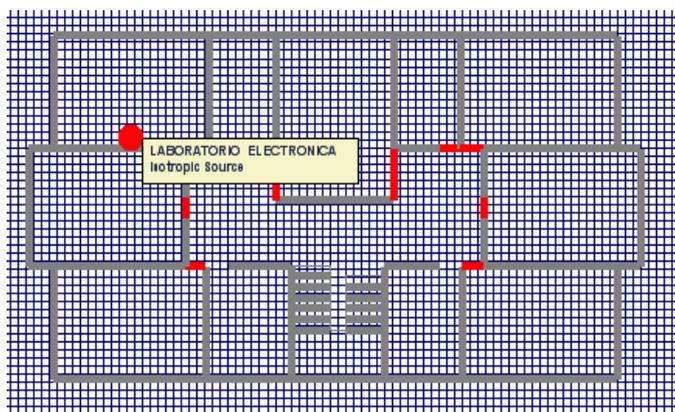


Propagación en 2D en Filosofía PISO 4

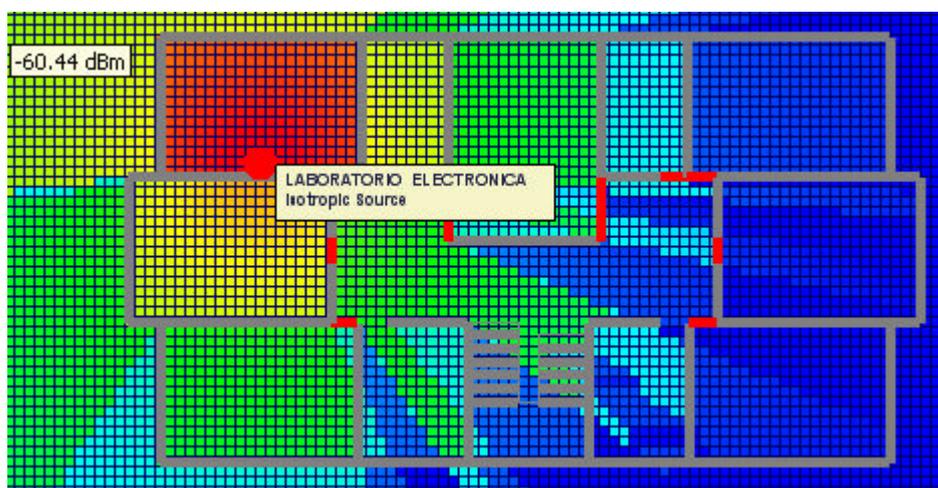


Propagación en 3D en Filosofía PISO 4

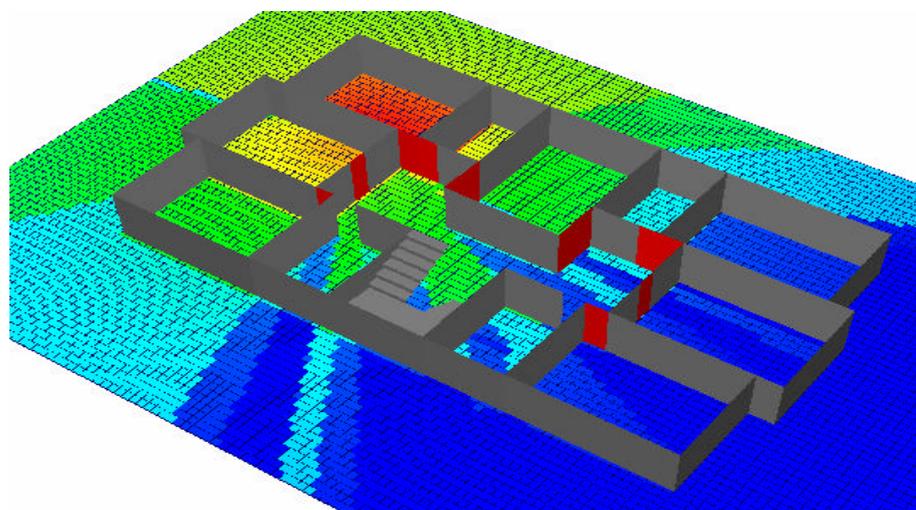
4.13 SIMULACIÓN DE LABORATORIO DE ELECTRONICA



Ubicación de Access Point y Plano del Lab. Electrónica

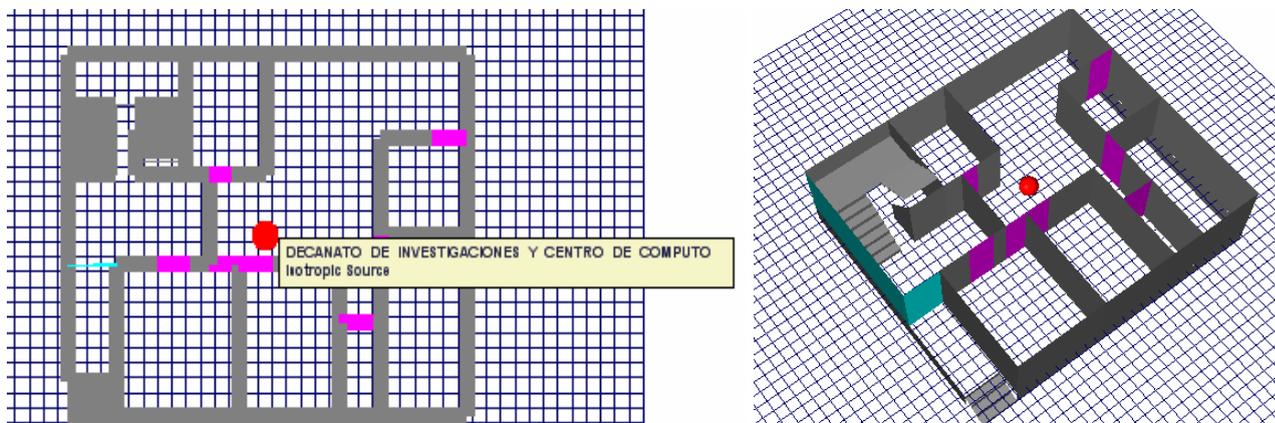


Propagación en 2D en Lab. Electrónica

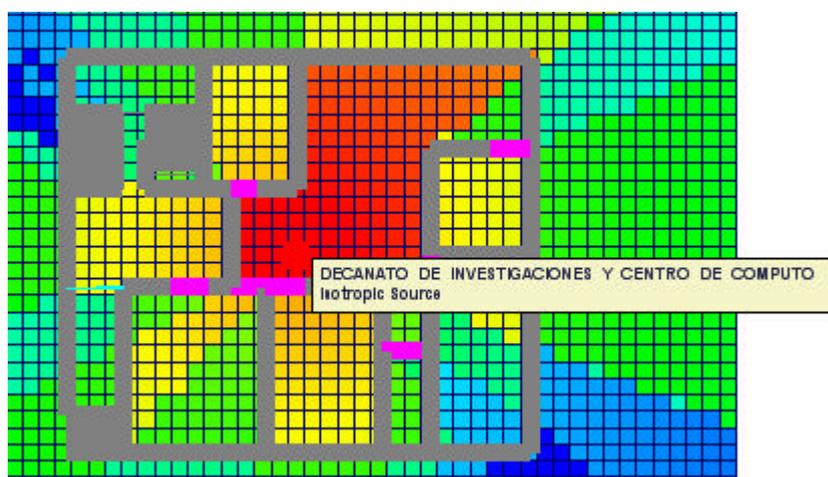


Propagación en 3D en Lab. Electrónica

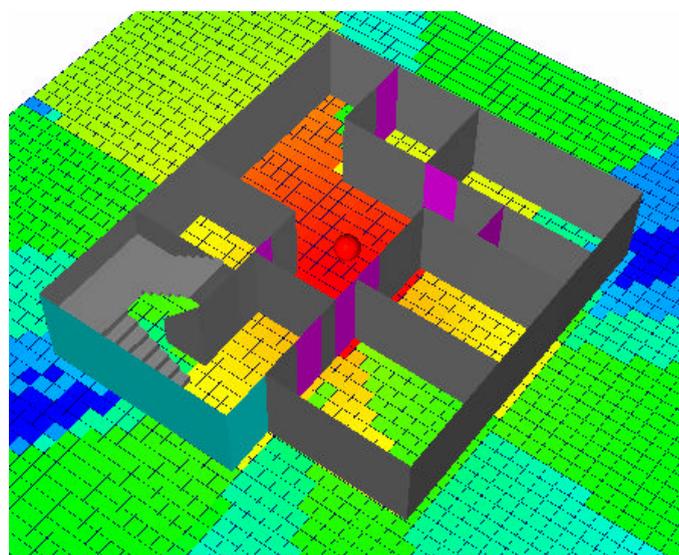
4.14 SIMULACIÓN DEL DECANATO DE INVESTIGACIONES Y CENTRO DE COMPUTO PLANTA BAJA



Ubicación de Access Point y Plano del IERCE Planta Baja

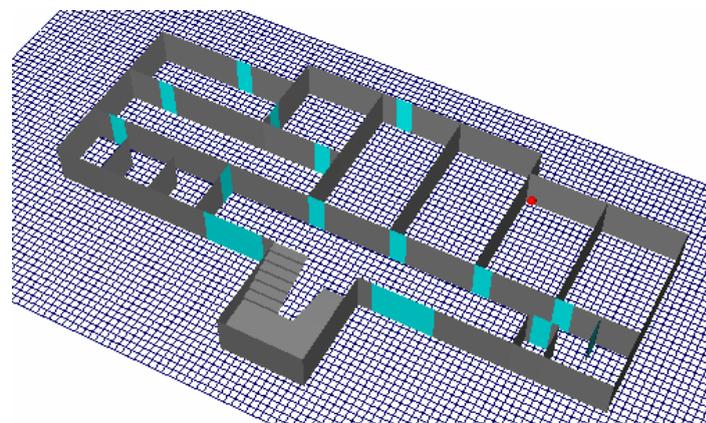
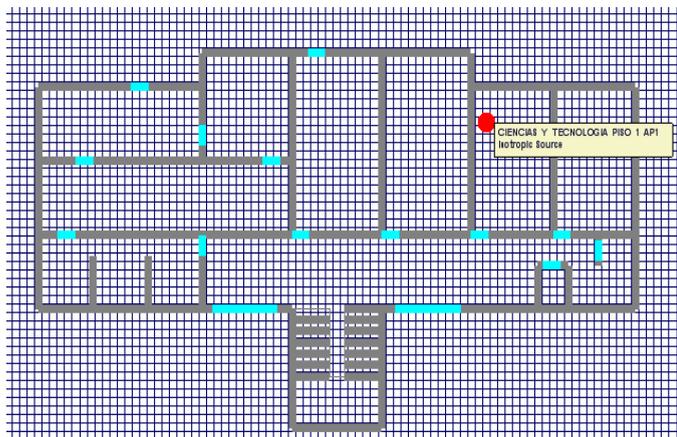


Propagación en 2D en IERCE Planta Baja

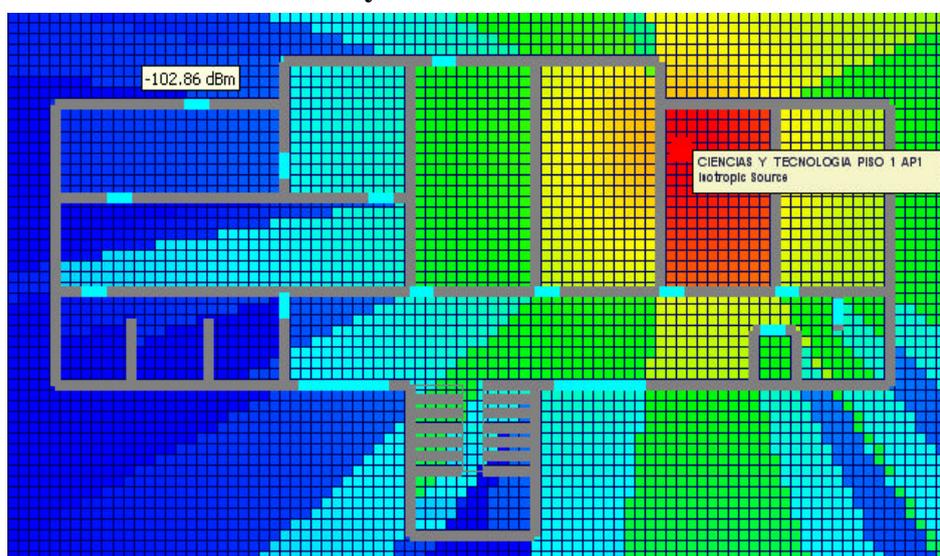


Propagación en 3D en IERCE Planta Baja

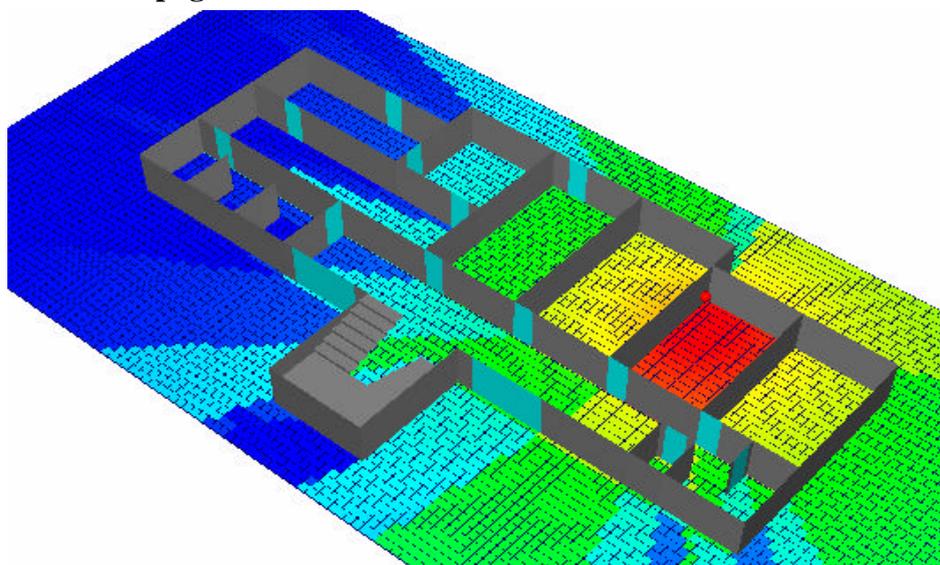
4.15 SIMULACIÓN DE LA FACULTAD DE CIENCIAS Y TECNOLOGÍA.



Ubicación de Access Point y Plano de CIENCIAS Y TECNOLOGÍA 1

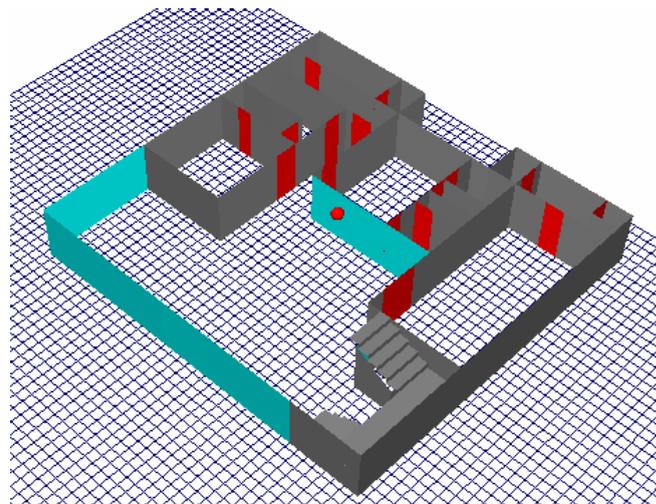
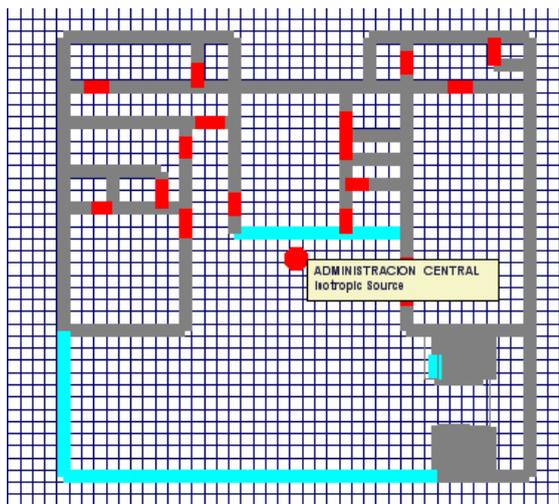


Propagación en 2D en CIENCIAS Y TECNOLOGÍA 1

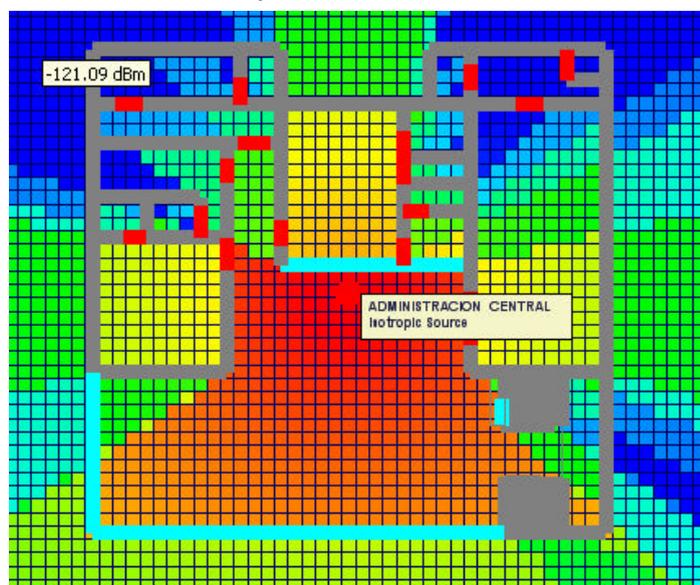


Propagación en 3D en CIENCIAS Y TECNOLOGÍA 1

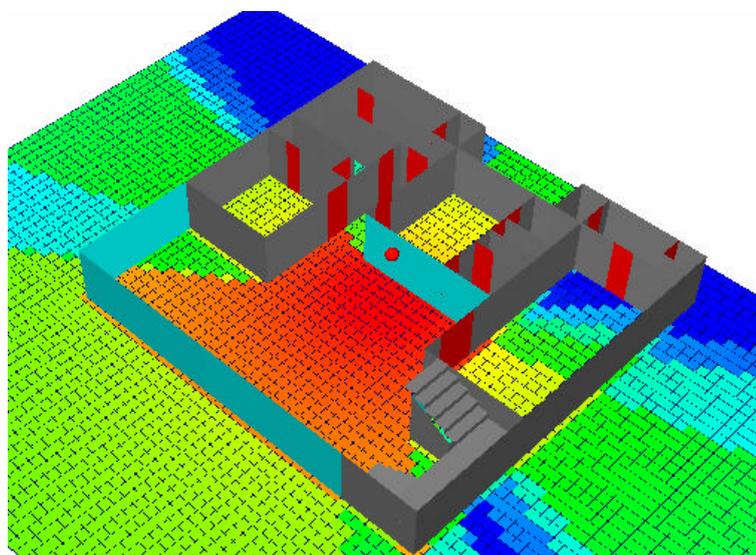
4.16 SIMULACIÓN DEL EDIFICIO DE ADMINISTRACIÓN CENTRAL



Ubicación de Access Point y Plano de la Administración Central

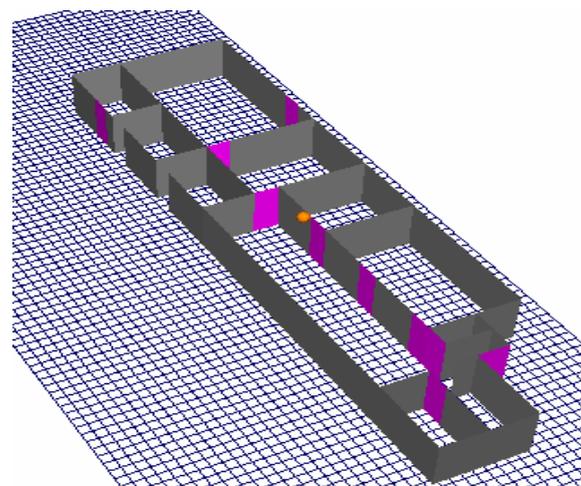
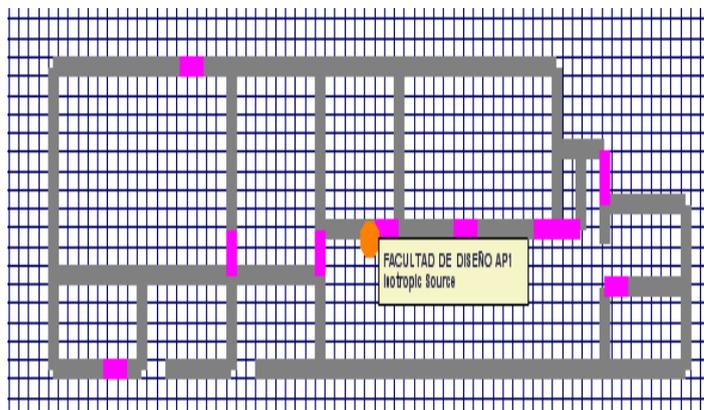


Propagación en 2D en la Administración Central

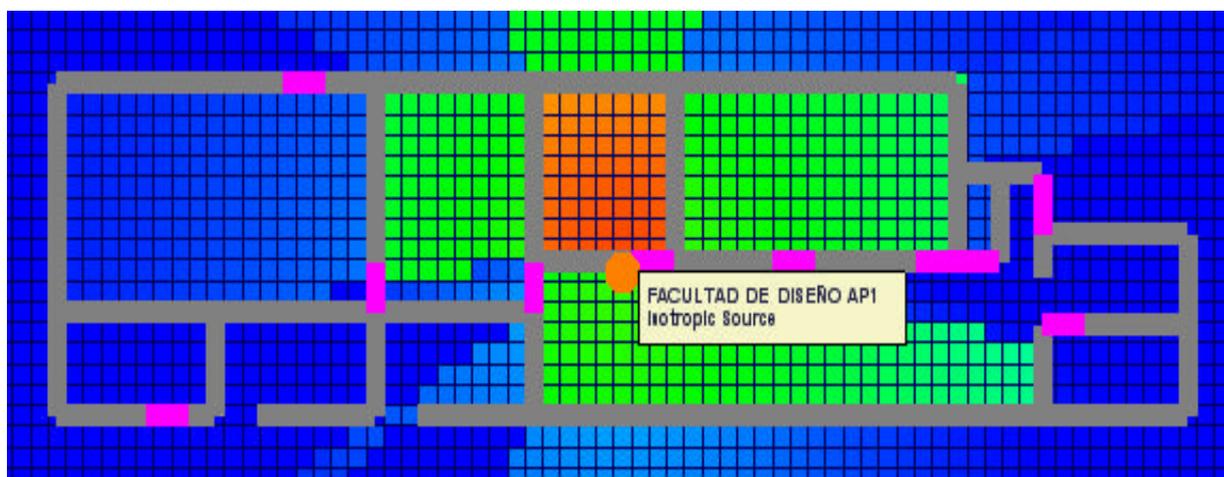


Propagación en 3D en la Administración Central

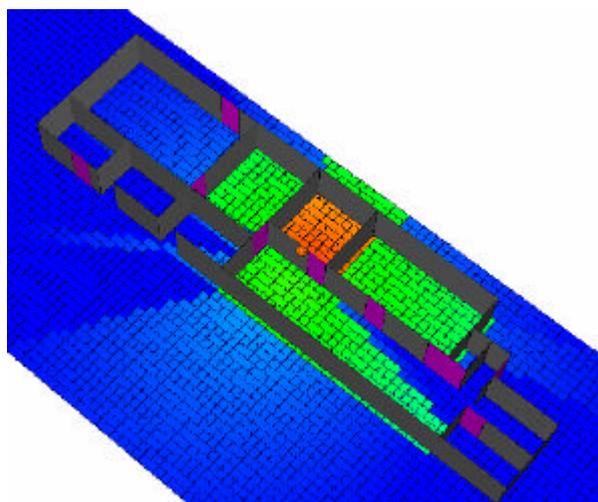
4.17 SIMULACIÓN DE LA FACULTAD DE DISEÑO



Ubicación de Access Point y Plano de la Facultad de Diseño

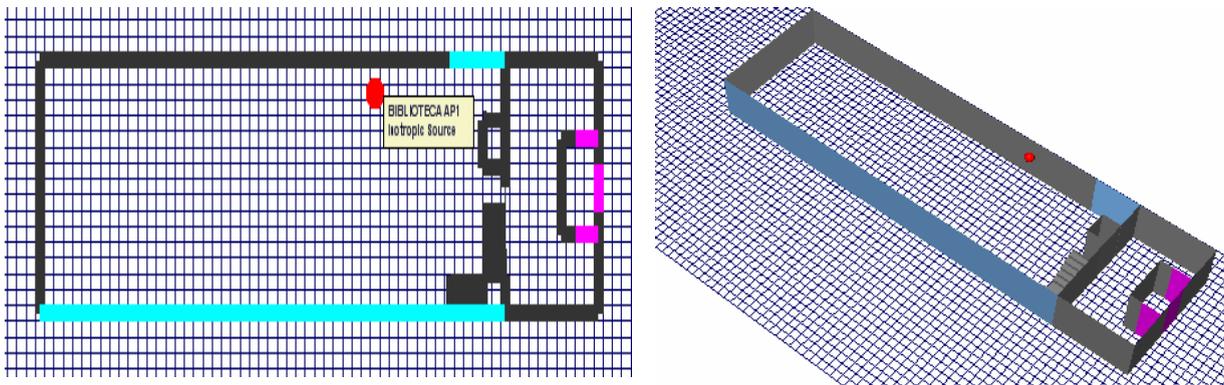


Propagación en 2D en la Facultad de Diseño

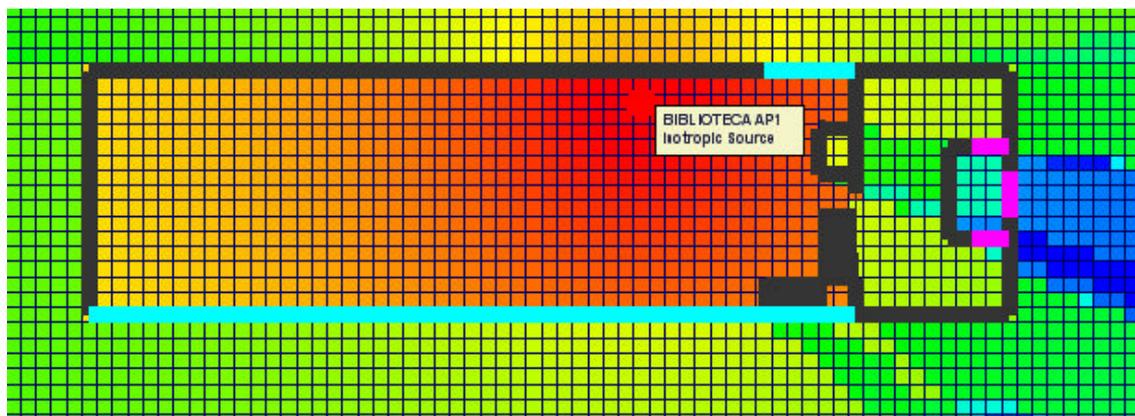


Propagación en 3D en la Facultad de Diseño

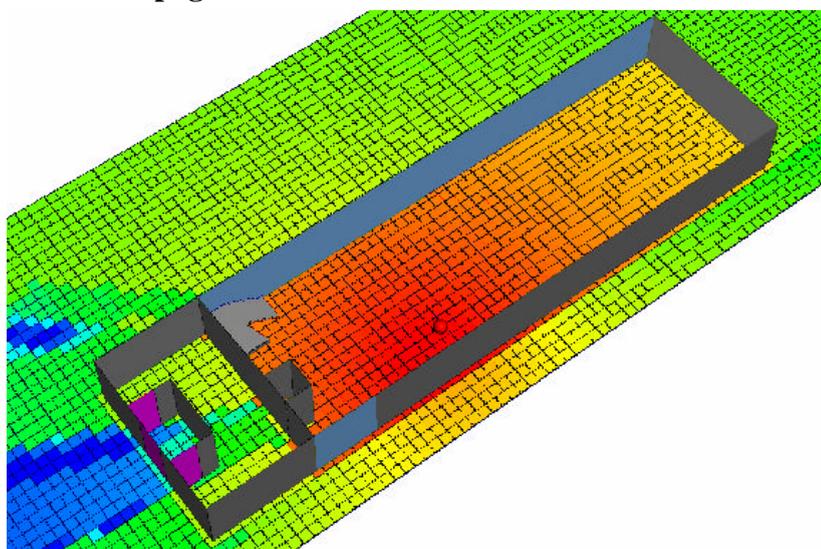
4.18 SIMULACIÓN DE LA IBLIOTECA.



Ubicación de Access Point y Plano de la Facultad de Diseño



Propagación en 2D en la Facultad de Diseño



Propagación en 3D en la Facultad de Diseño

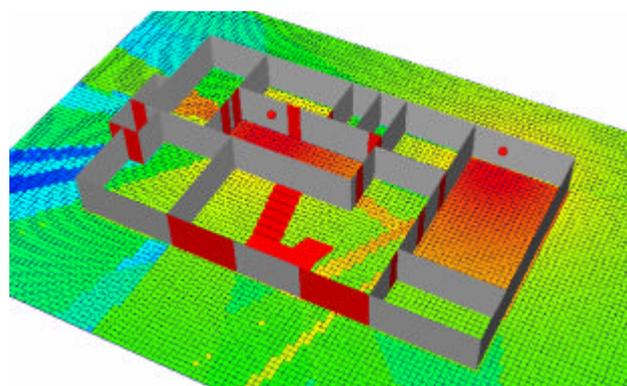
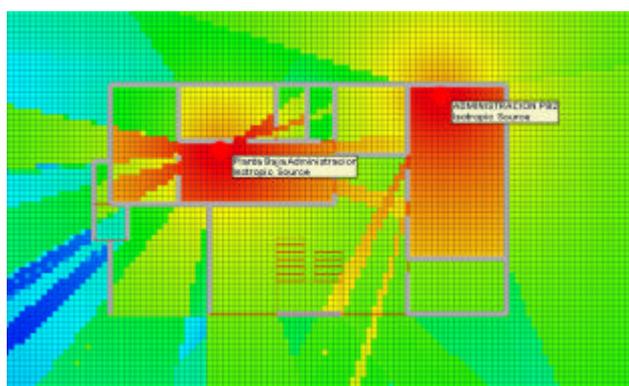
Como se puede apreciar en todas las simulaciones realizadas se obtiene la realidad existente en la universidad, se puede apreciar que existen lugares en donde no se esta obteniendo una cobertura adecuada como en el edificio de administración, el edificio de filosofía, en donde las paredes no permiten que se tenga un valor de campo adecuado para poder tener las velocidades y los servicios que la red WIFI nos puede brindar.

4.19 PROPUESTA DE UBICACIÓN Y MEJORAMIENTO DE AREAS DE COBERTURA EN CADA SECTOR DE LA UDA.

Se realizara el desarrollo de una propuesta para mejorar la cobertura y la propagación dentro de cada sector de la Universidad, se tomara en cuenta la reubicación y la instalación de Access Point en donde obtendremos los siguientes resultados:

4.19.1 ADMINISTRACION PLANTA BAJA

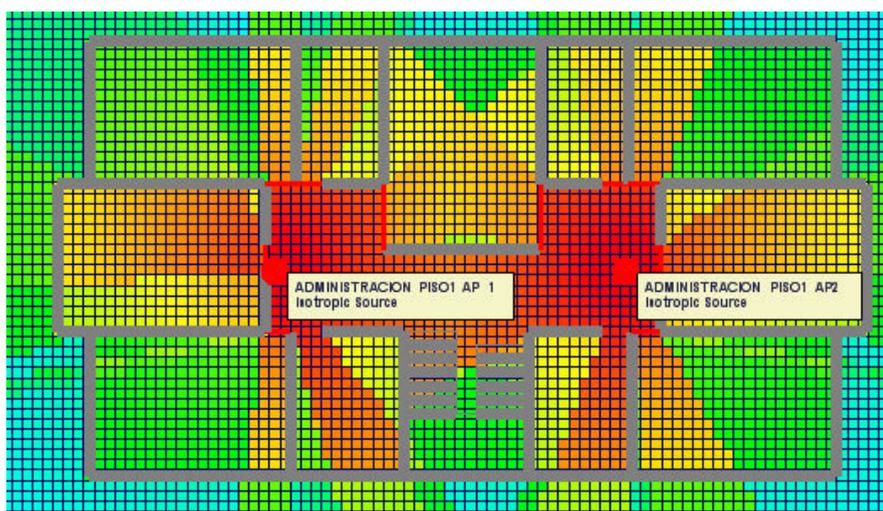
En este lugar bs Access Point se encuentran ubicados de manera adecuada ya que la cobertura que se tiene da la posibilidad que los usuarios tengan un valor de campo requerido y puedan ingresar a la red WIFI sin problemas de velocidad y ancho de banda ofrecido.



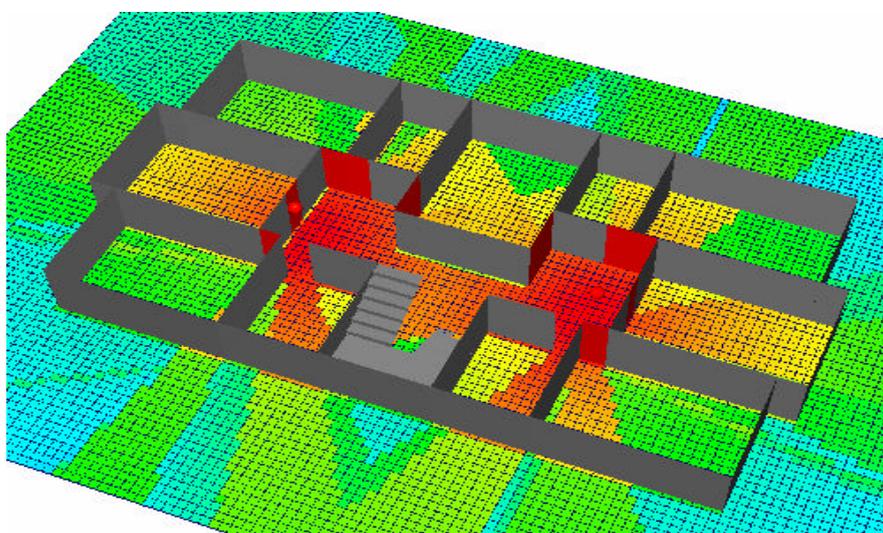
Ubicación de Access Point en Administración Planta Baja

4.19.2 ADMINISTRACION PISO 1

Para este sector se necesita la reubicación del Access Point existente he incorporar otro ya que el área en donde esta concentrado la cobertura son los pasillos como se vio anteriormente, razón por la cual no se tiene un correcto valor de campo en la parte interior de las aulas, de acuerdo a ese concepto se debe ubicar los Access Point como se ve a continuación.



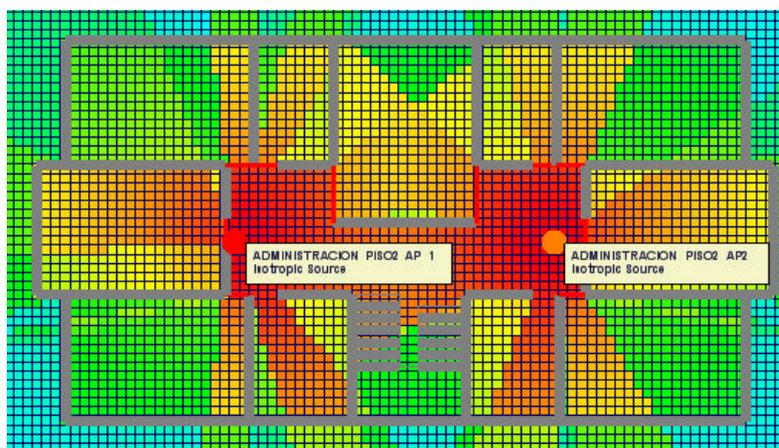
Propagación Mejorada con 2 Access Point en 2D



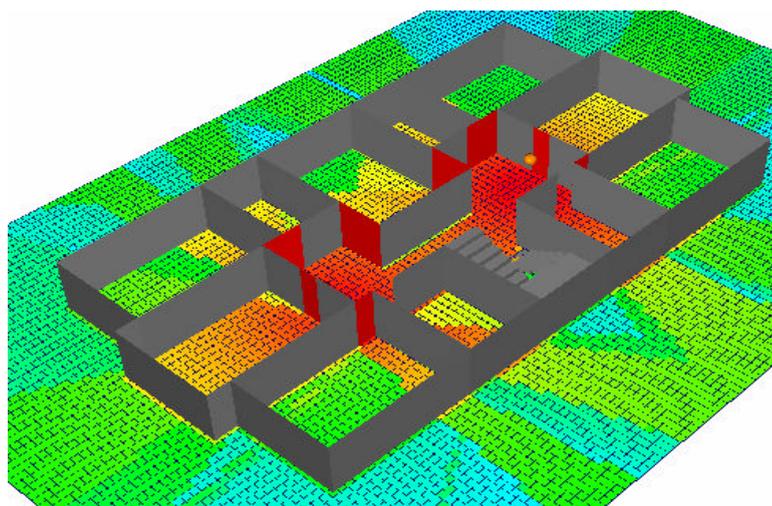
Propagación Mejorada con 2 Access Point en 3D

4.19.3 ADMINISTRACION PISO 2

Para este sector se debe tomar en cuenta el criterio del piso 1



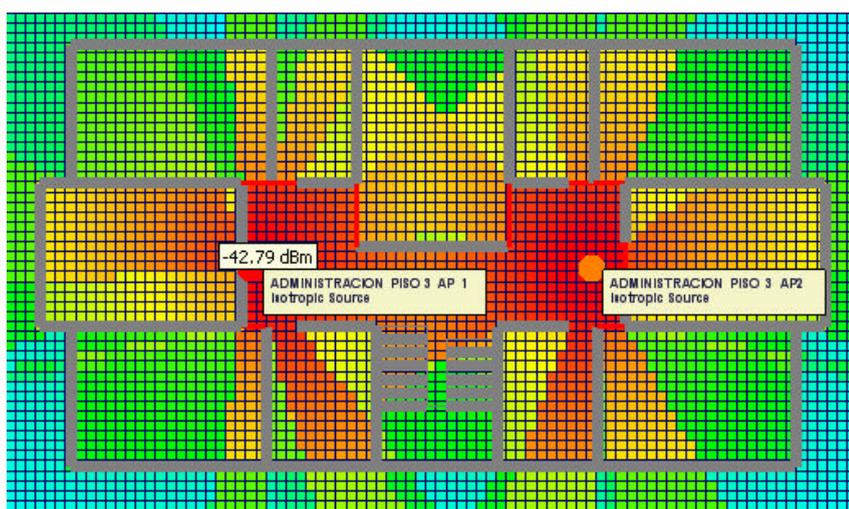
Propagación Mejorada con 2 Access Point en 2D



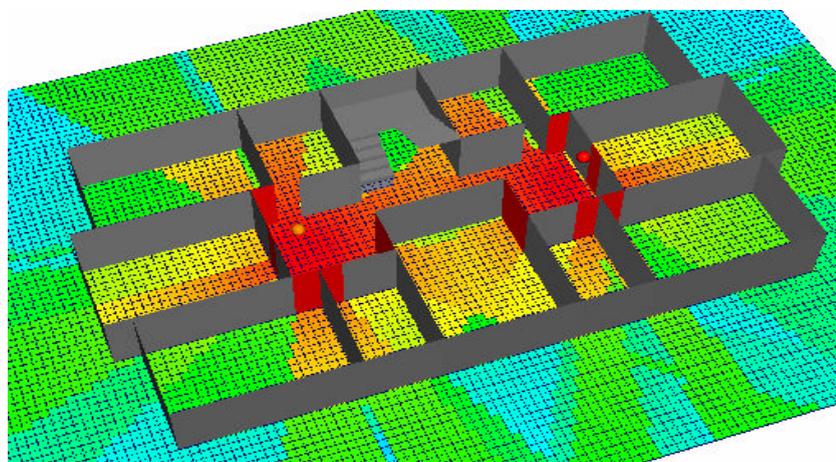
Propagación Mejorada con 2 Access Point en 3D

4.19.4 ADMINISTRACION PISO 3

Para este sector se debe tomar en cuenta el criterio del piso 1



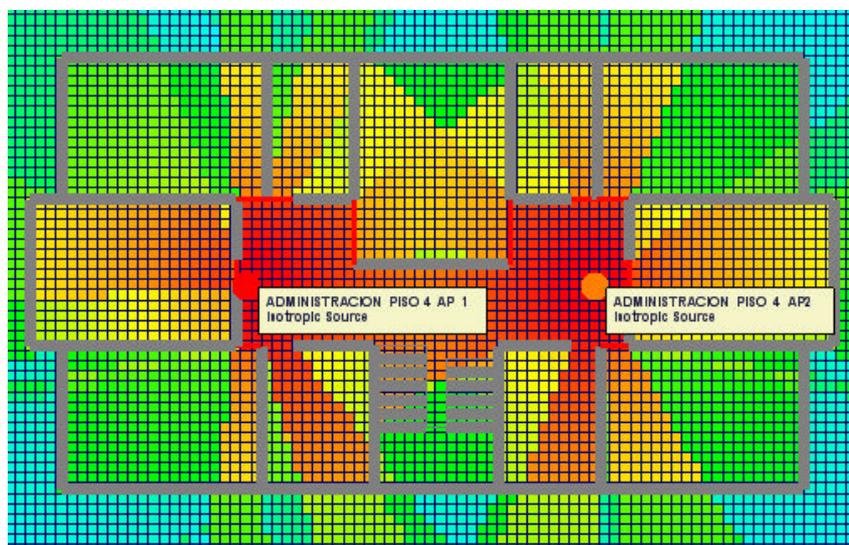
Propagación Mejorada con 2 Access Point en 2D



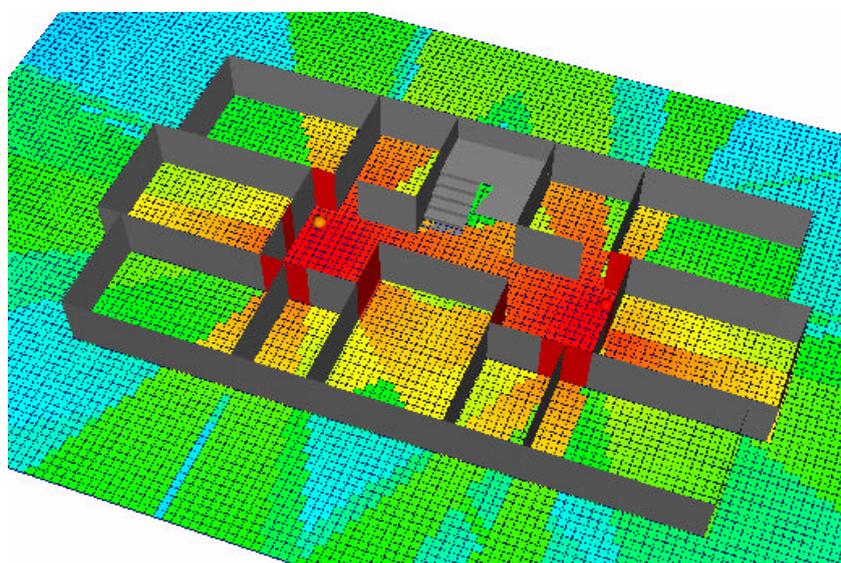
Propagación Mejorada con 2 Access Point en 3D

4.19.5 ADMINISTRACION PISO 4

Para este sector se debe tomar en cuenta el criterio del piso 1.



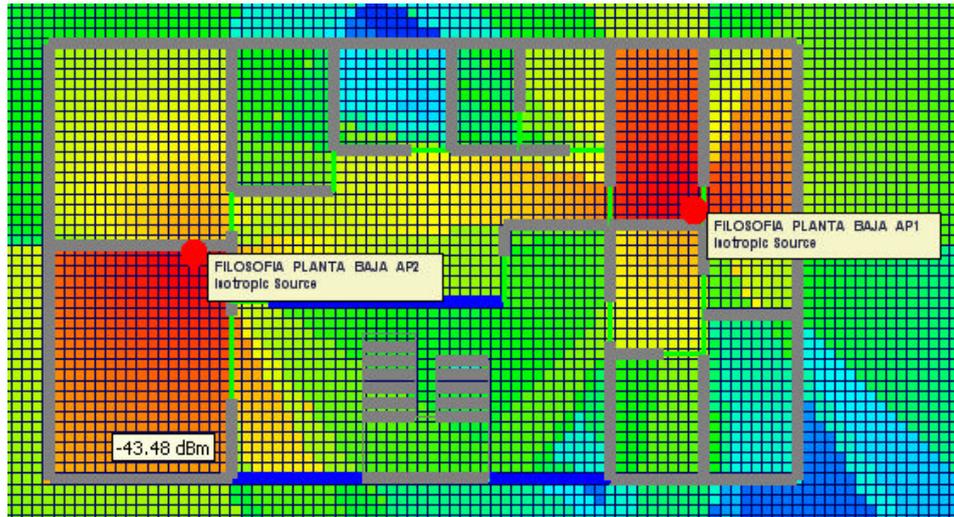
Propagación Mejorada con 2 Access Point en 2D



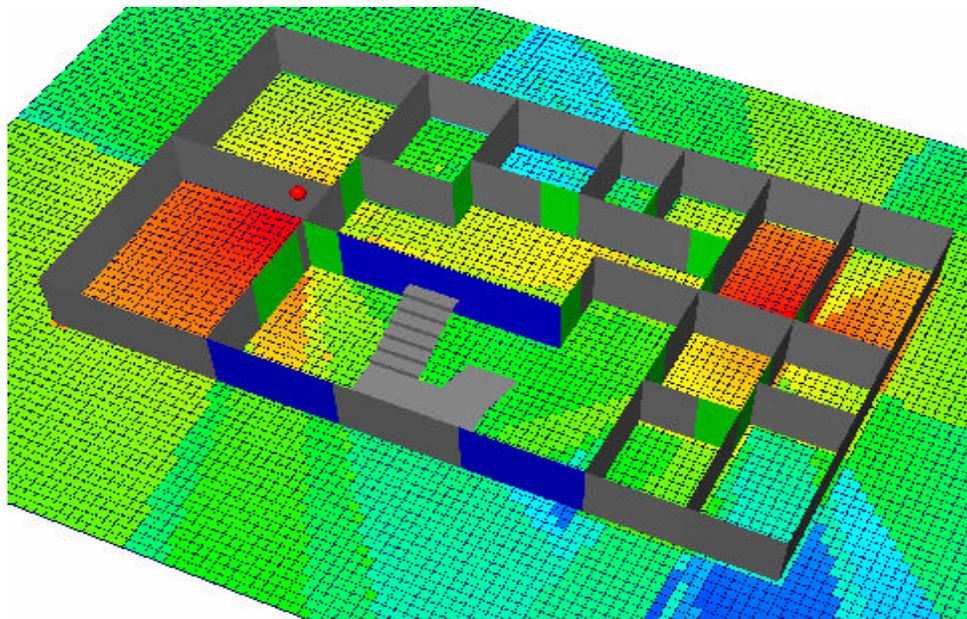
Propagación Mejorada con 2 Access Point en 3D

4.19.6 FILOSOFIA PLANTA BAJA

Para este sector se necesita la reubicación del Access Point existente he incorporar otro ya que el área en donde esta concentrado la cobertura es el pasillo como se vio en el estado actual, razón por la cual no se tiene un correcto valor de campo en la parte interior, de acuerdo a ese concepto se debe ubicar los Access Point como se ve a continuación, esto permitirá tener una mejor cobertura.



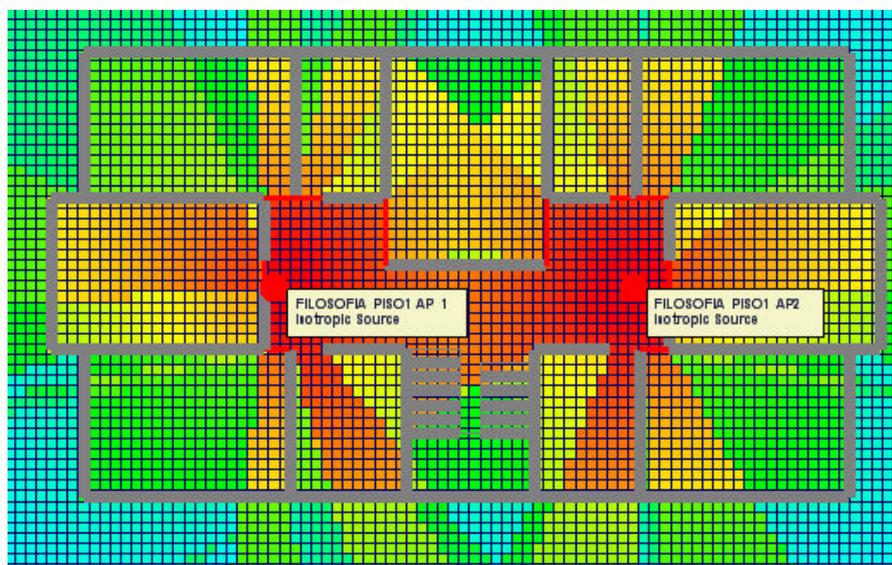
Propagación Mejorada con 2 Access Point en 2D



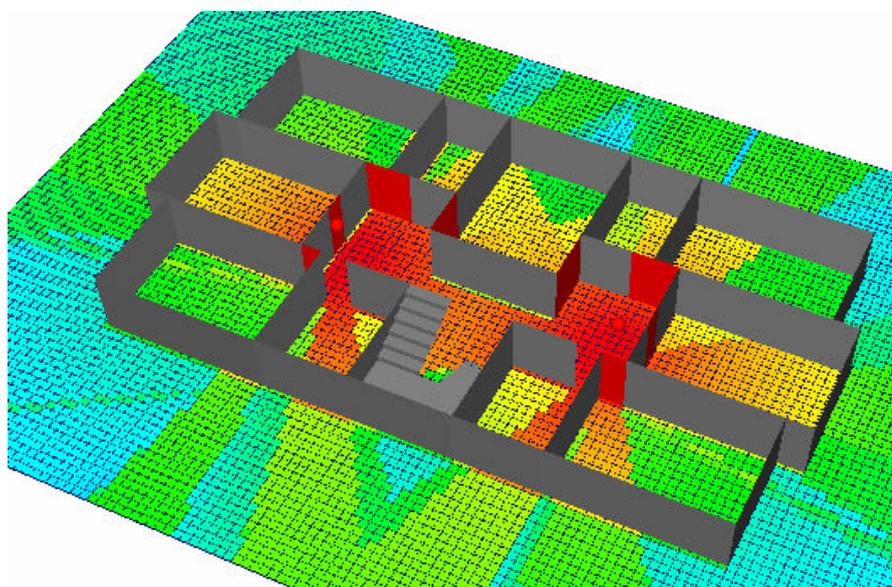
Propagación Mejorada con 2 Access Point en 3D

4.19.7 FILOSOFIA PISO 1

Para este sector se debe tomar en cuenta el criterio que se dio en la planta baja y se ve la mejora en la propagación dentro de las aulas



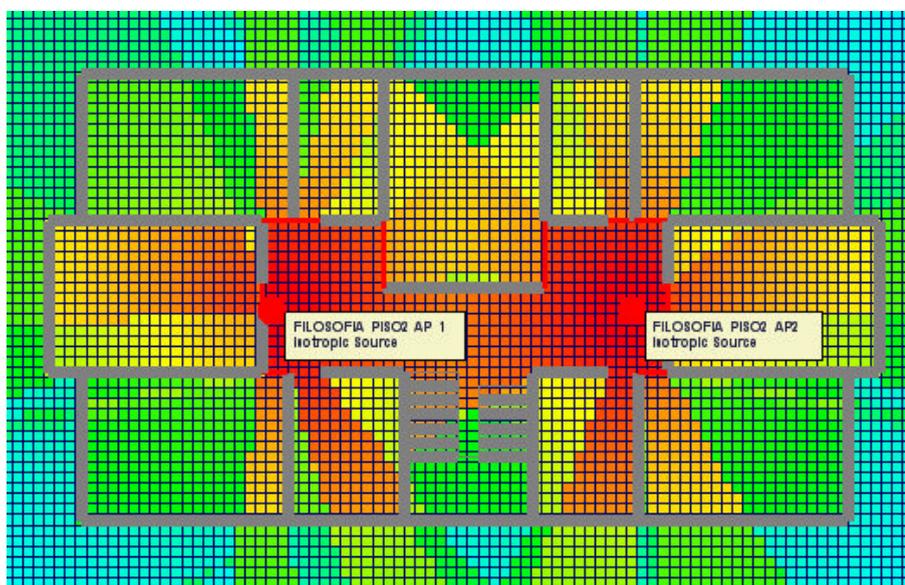
Propagación Mejorada con 2 Access Point en 2D



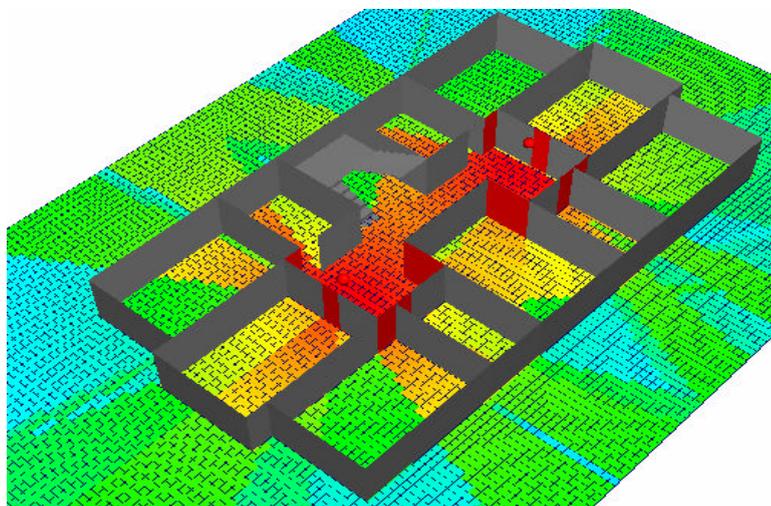
Propagación Mejorada con 2 Access Point en 3D

4.19.8 FILOSOFIA PISO 2

Para este sector se debe tomar en cuenta el criterio que se dio en la planta baja y se ve la mejora en la propagación dentro de las aulas



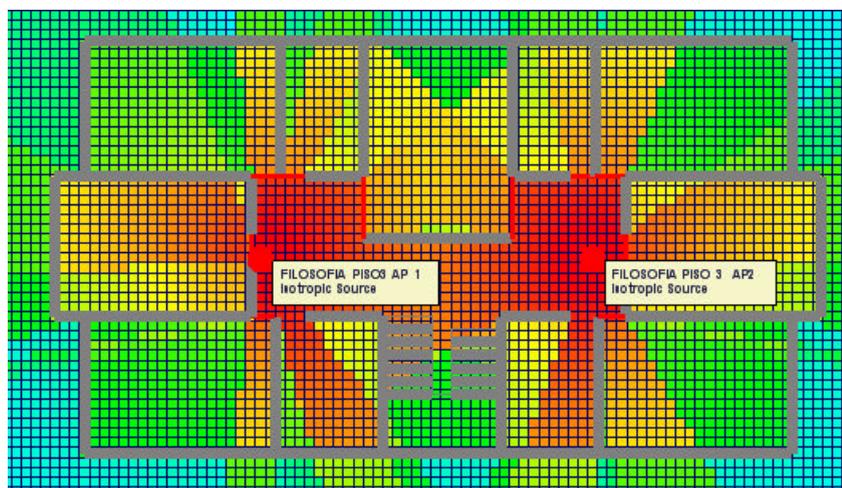
Propagación Mejorada con 2 Access Point en 2D



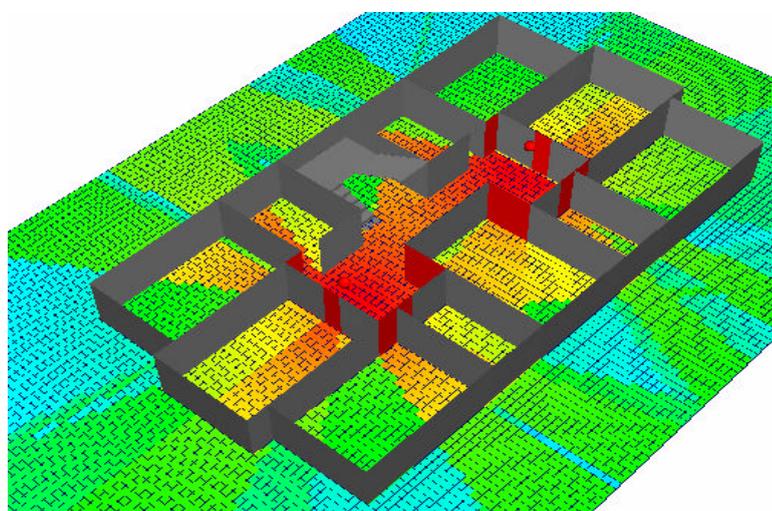
Propagación Mejorada con 2 Access Point en 3D

4.19.9 FILOSOFIA PISO 3

Para este sector se debe tomar en cuenta el criterio que se dio en la planta baja y se ve la mejora en la propagación dentro de las aulas



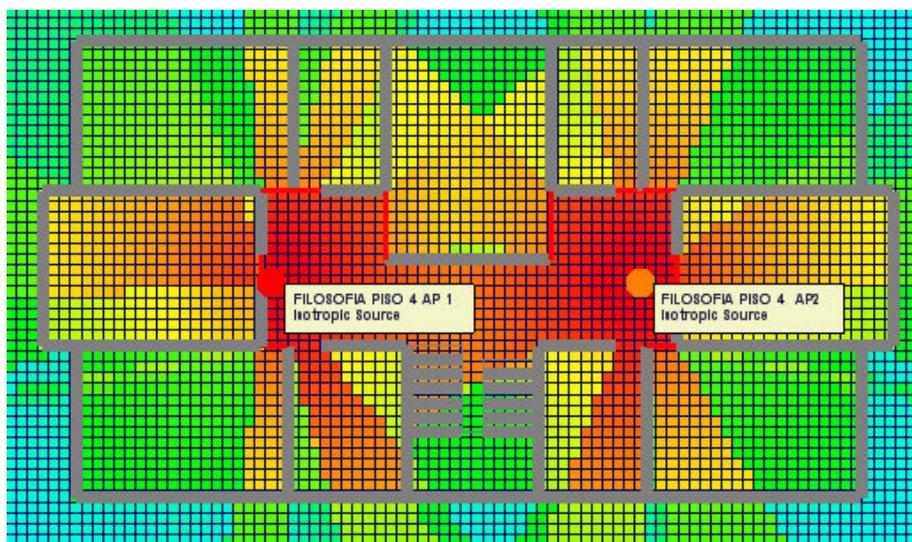
Propagación Mejorada con 2 Access Point en 2D



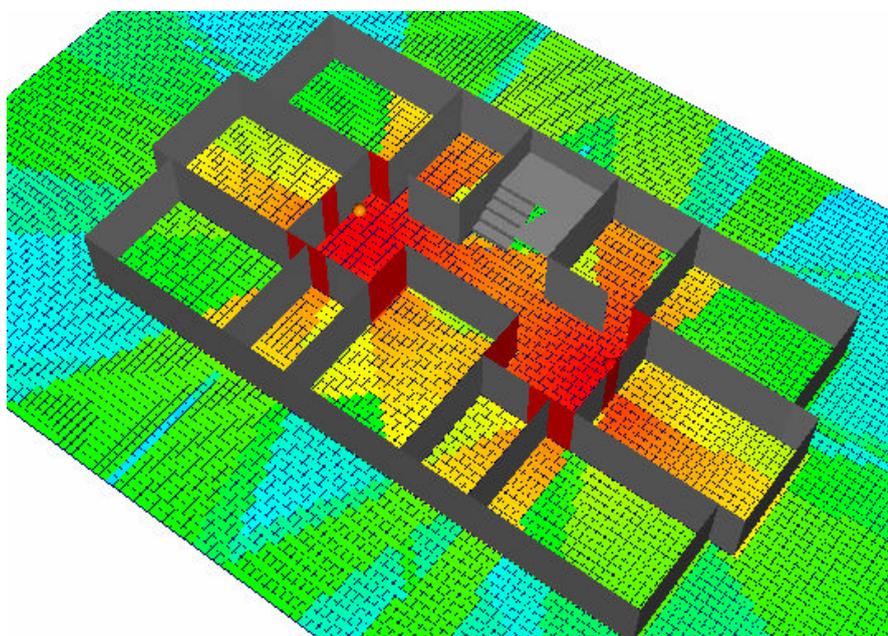
Propagación Mejorada con 2 Access Point en 3D

4.19.10 FILOSOFIA PISO 4

Para este sector se debe tomar en cuenta el criterio que se dio en la planta baja y se ve la mejora en la propagación dentro de las aulas

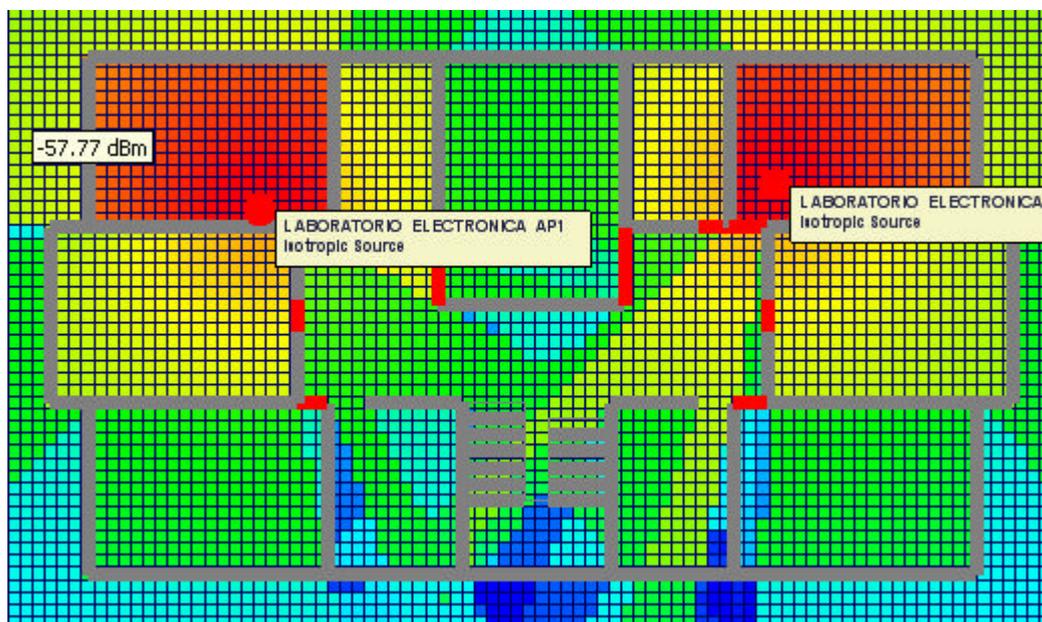


Propagación Mejorada con 2 Access Point en 2D

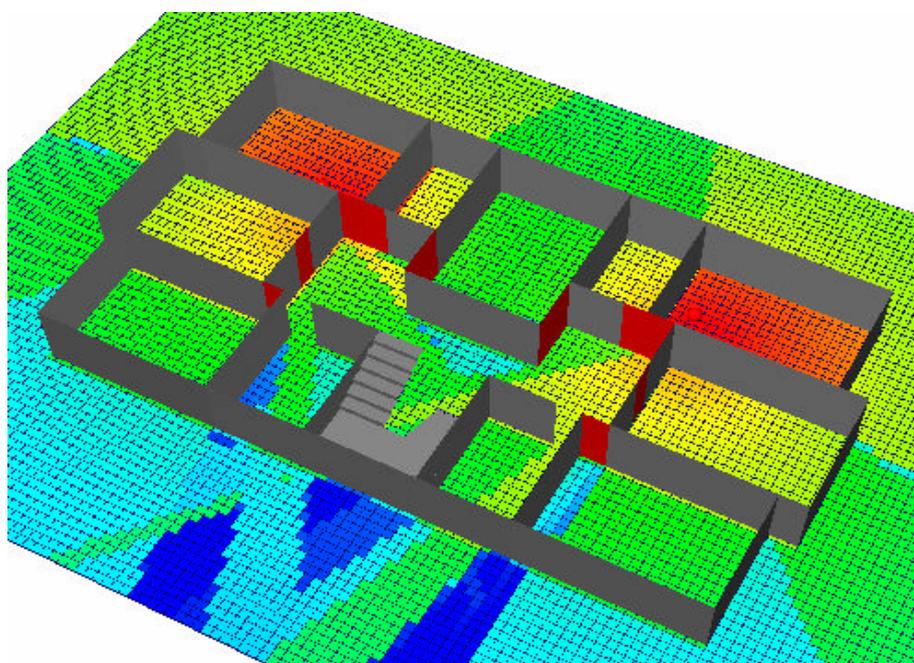


Propagación Mejorada con 2 Access Point en 3D

4.19.11 LABORATORIO DE ELECTRONICA



Propagación Mejorada con 2 Access Point en 2D

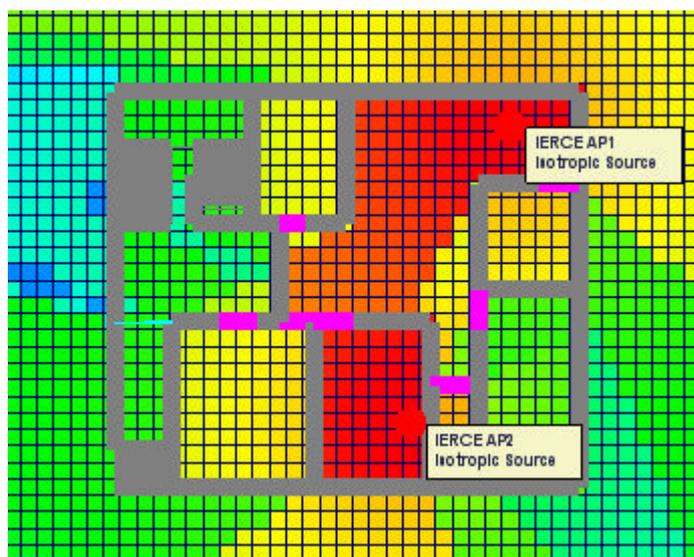


Propagación Mejorada con 2 Access Point en 3D

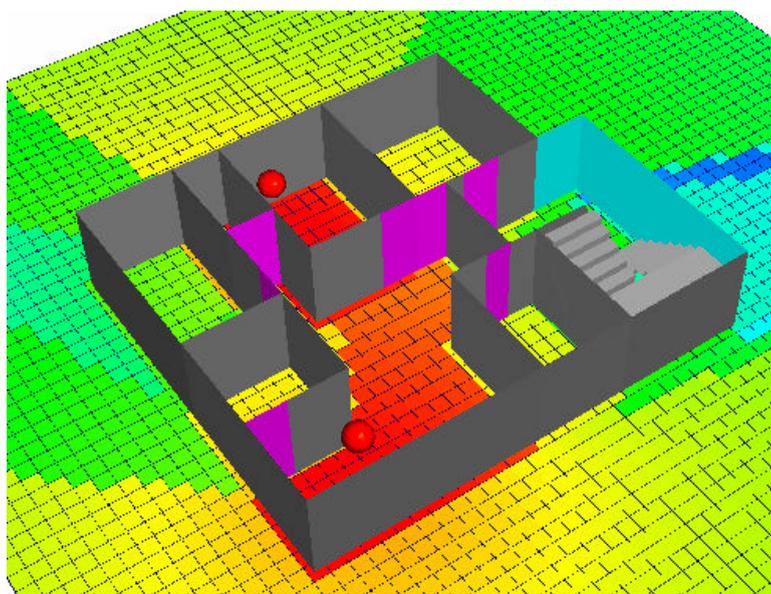
4.19.12 DECANATO DE INVESTIGACIONES Y CENTRO DE COMPUTO PLANTA BAJA

Para este lugar se tiene que ubicar en cada planta un Access Point para de esta manera cubrir correctamente el área de servicio hacia los usuarios, a continuación se detalla cada uno de los pisos y la localización de Access Point en todo el IERCE

PLANTA BAJA

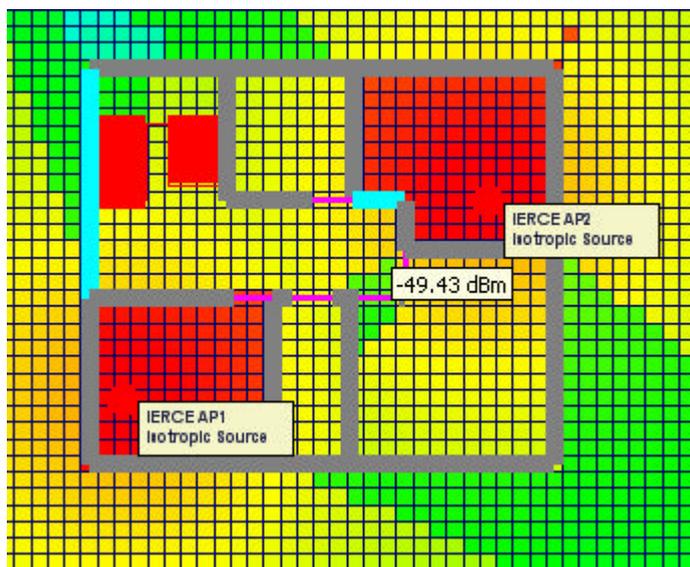


Ubicación de Access Point y Plano del IERCE Planta Baja

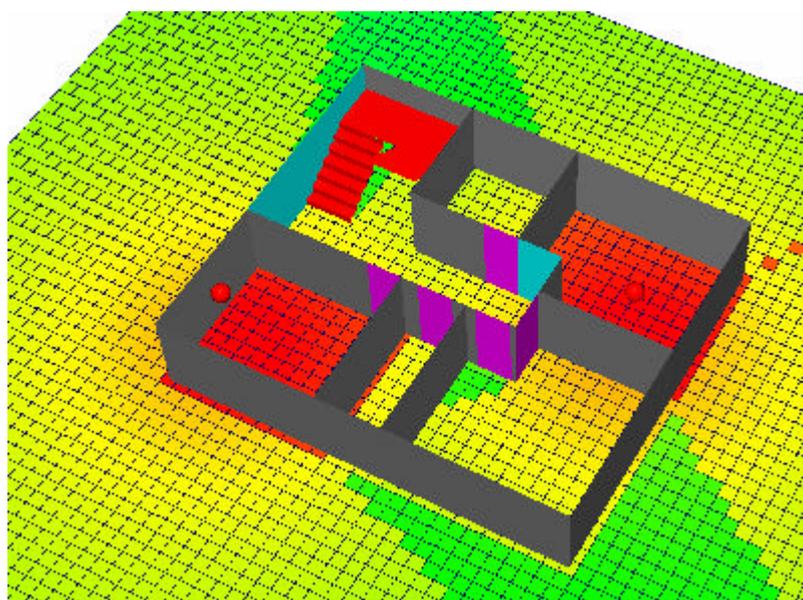


Propagación en 3D en IERCE Planta Baja

PLANTA PISO 1

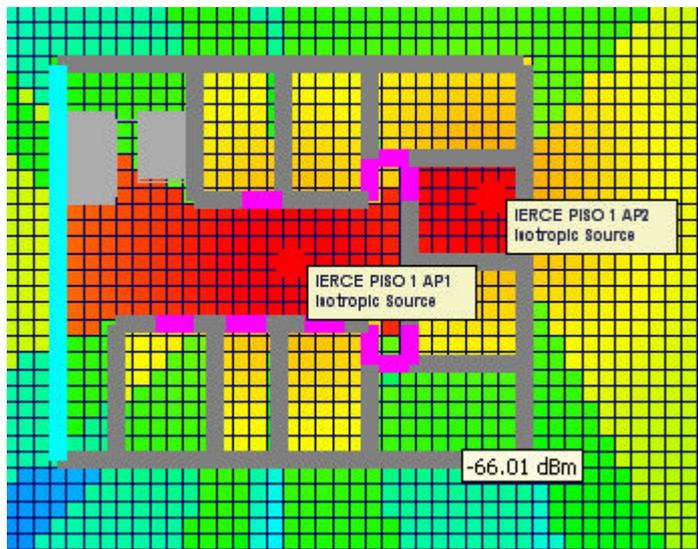


Ubicación de Access Point y Plano del IERCE PISO 1

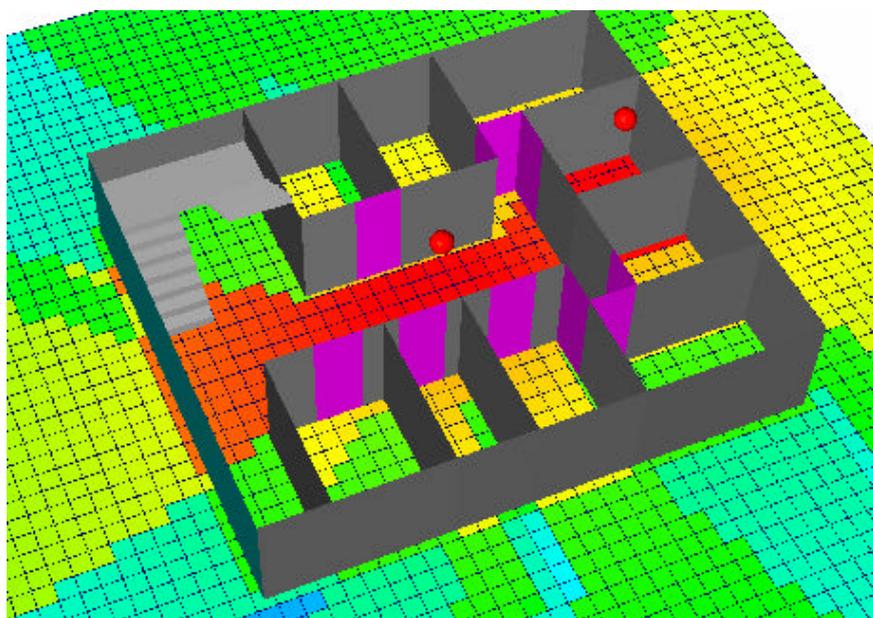


Propagación en 3D en IERCE PISO 1

PLANTA PISO 2



Ubicación de Access Point y Plano del IERCE PISO 2



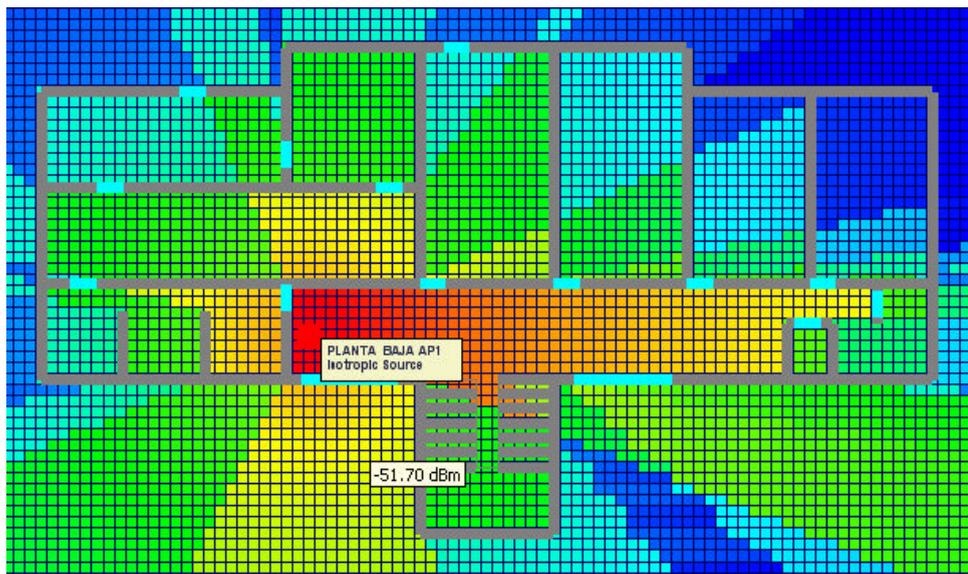
Propagación en 3D en IERCE PISO 2

4.19.13 FACULTAD DE CIENCIAS Y TECNOLOGÍA.

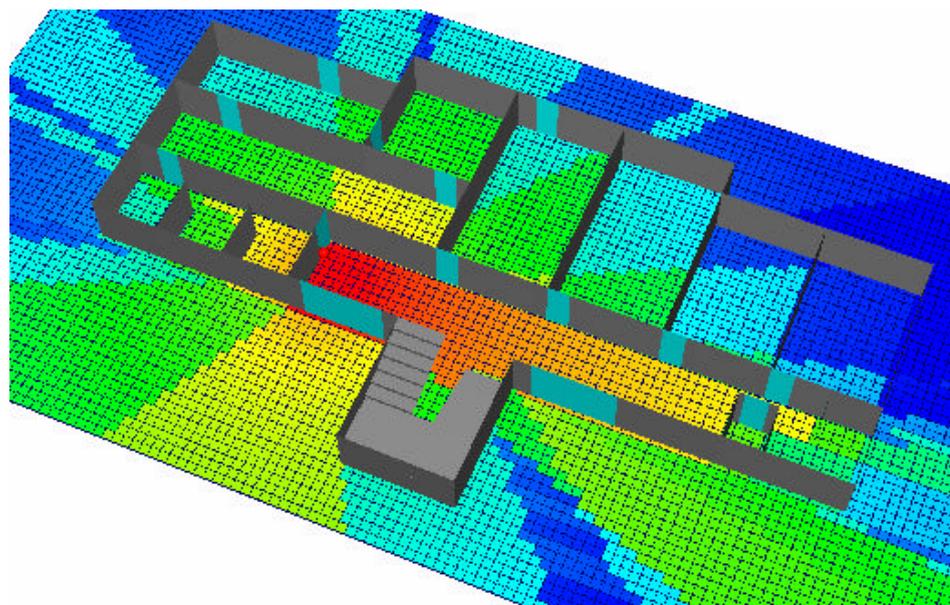
Esta facultad necesita aumentar una buena cantidad de Access Point para poder mejorar su cobertura, para cada planta se a diseñado utilizar una mejor disposición de los equipos como se ve a continuación:

PLANTA BAJA

En esta planta se debe instalar un Access Point que nos cubra la parte exterior de mejor manera para que los usuarios se puedan conectar desde el exterior a la red.



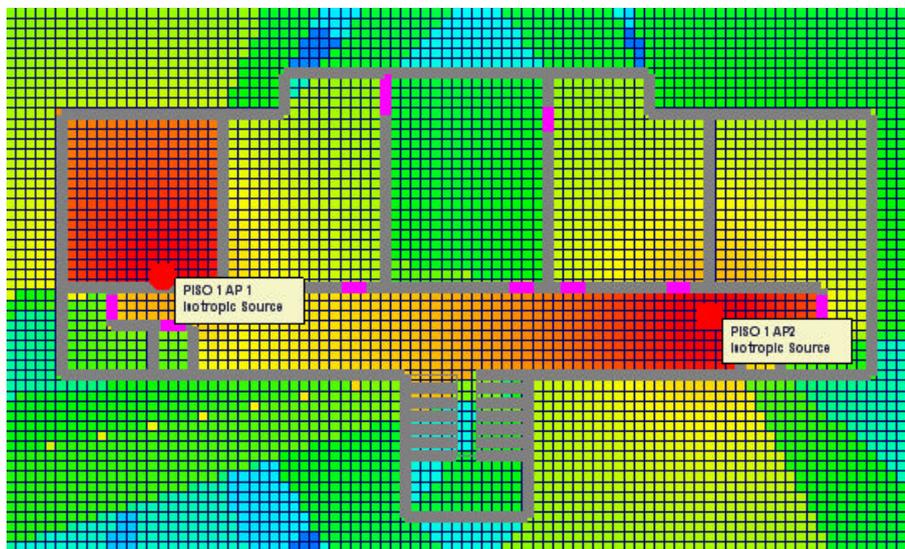
Ubicación de Access Point y Plano en CIENCIAS Y TECNOLOGÍA Planta Baja



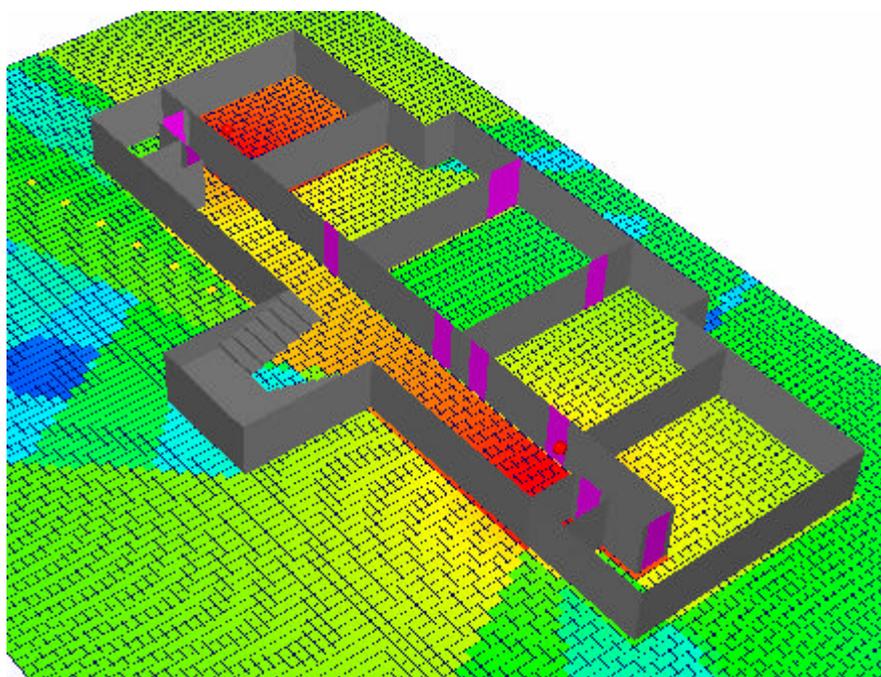
Propagación en 3D en CIENCIAS Y TECNOLOGÍA Planta Baja

PISO 1

En esta planta se debe instalar un access point Adicional para poder cubrir las aulas y el pasillo del interior del edificio.



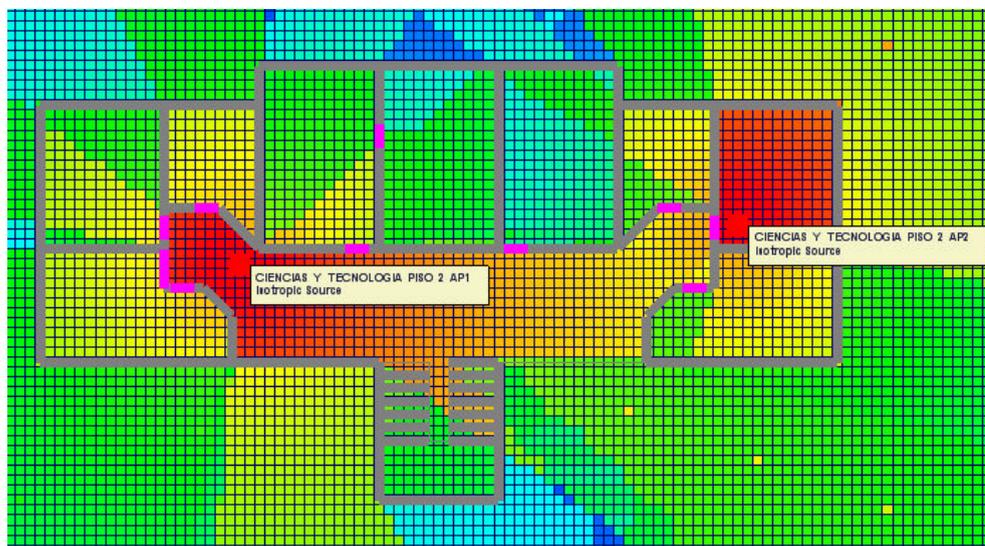
Ubicación de Access Point y Plano en CIENCIAS Y TECNOLOGÍA Piso 1



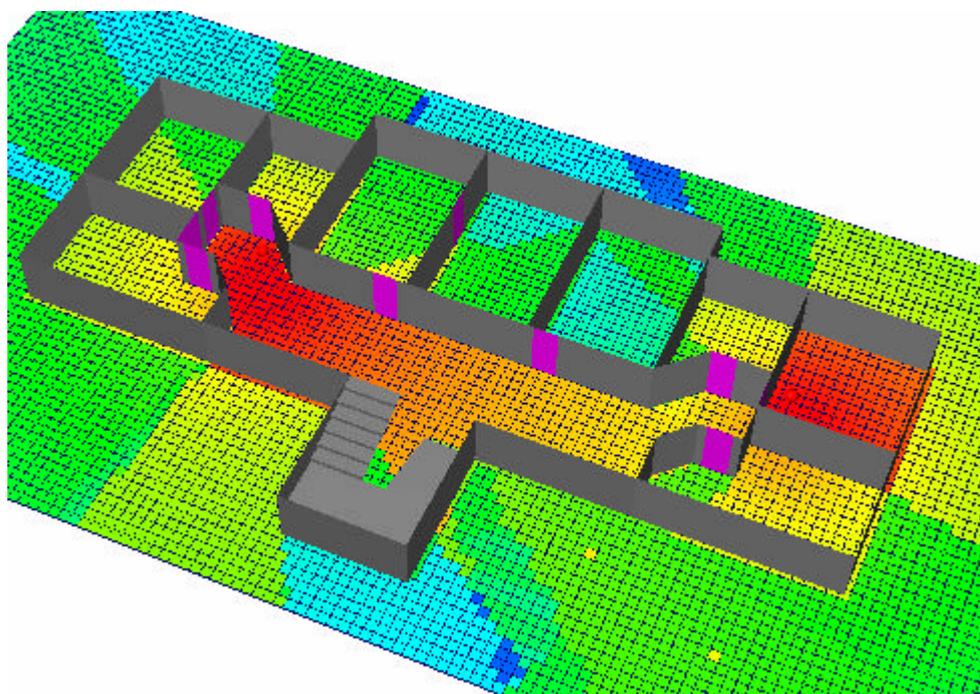
Propagación en 3D en CIENCIAS Y TECNOLOGÍA Piso 1

PISO 2

En esta planta se debe instalar un access point adicional para poder cubrir las aulas y el pasillo del interior del edificio.



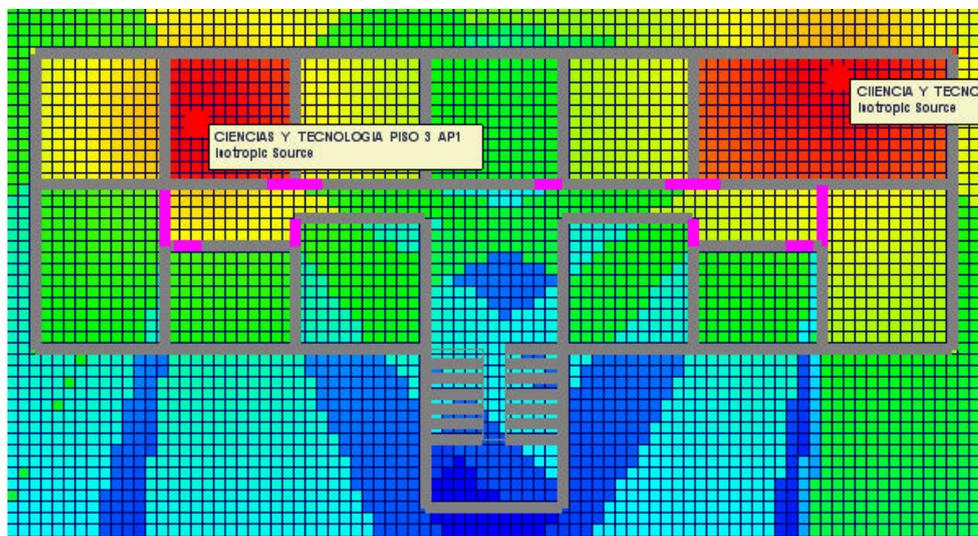
Ubicación de Access Point y Plano en CIENCIAS Y TECNOLOGÍA Piso 2



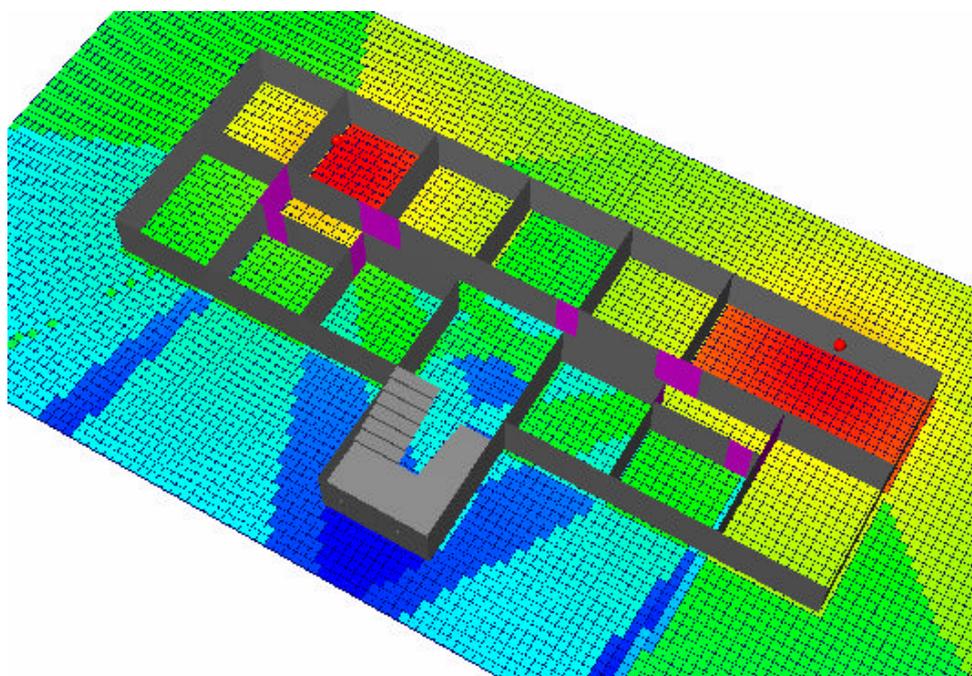
Propagación en 3D en CIENCIAS Y TECNOLOGÍA Piso 2

PISO 3

En esta planta se debe instalar un access point adicional para poder cubrir las aulas y el pasillo del interior del edificio.



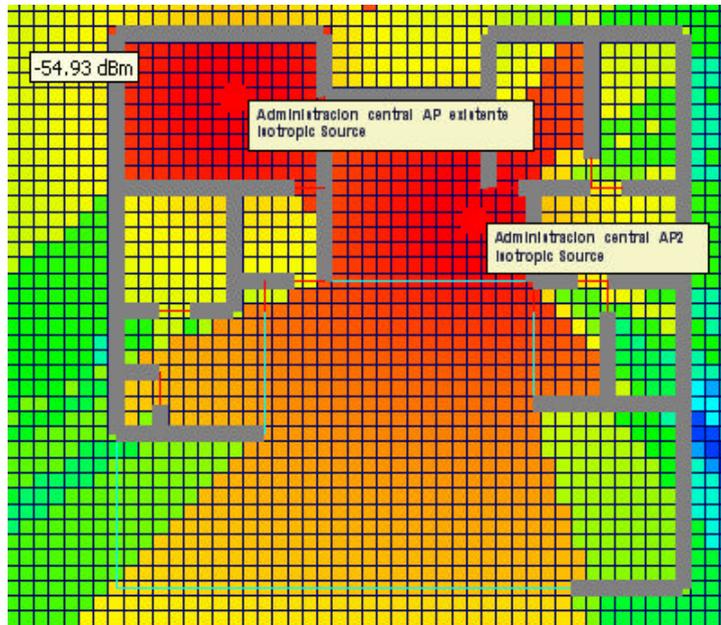
Ubicación de Access Point y Plano en CIENCIAS Y TECNOLOGÍA Piso 3



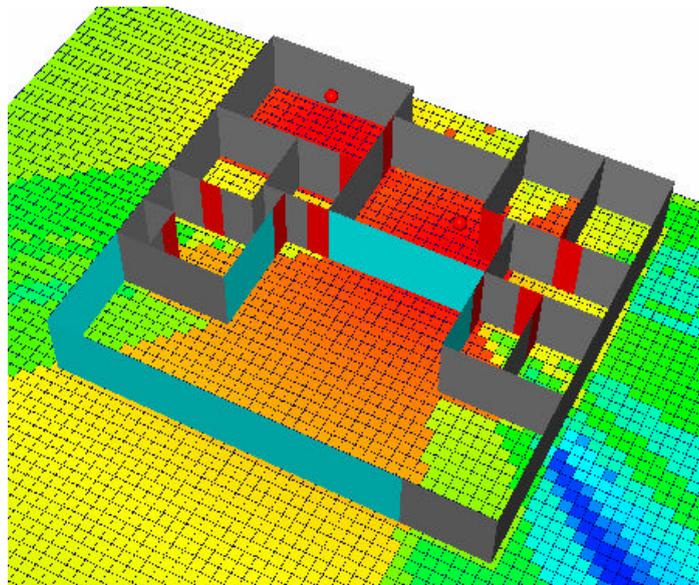
Propagación en 3D en CIENCIAS Y TECNOLOGÍA Piso 3

4.19.14 EDIFICIO DE ADMINISTRACIÓN CENTRAL

En este lugar la cantidad de usuarios puede variar ya que podrían conectarse a la red desde la parte exterior, teniendo una potencia en la señal adecuada y una velocidad optima, para esto se a dispuesto los Access Point de la siguiente manera.



Ubicación de Access Point y Plano en ADMINISTRACION CENTRAL Piso 3



Propagación en 3D en ADMINISTRACION CENTRAL Piso 3

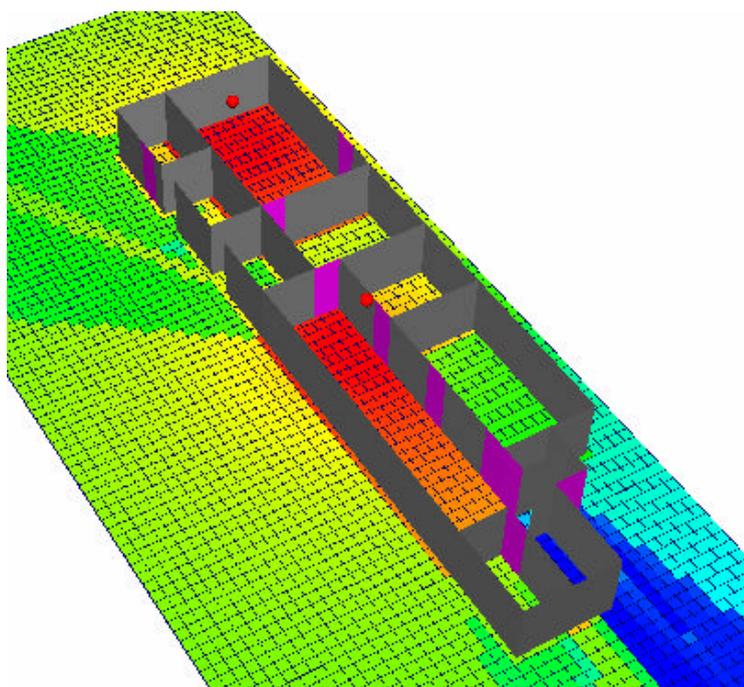
4.19.15 FACULTAD DE DISEÑO

DISEÑO PLANTA BAJA

En esta planta se debe instalar un access point adicional para poder cubrir las areas en donde se requiere cobertura.



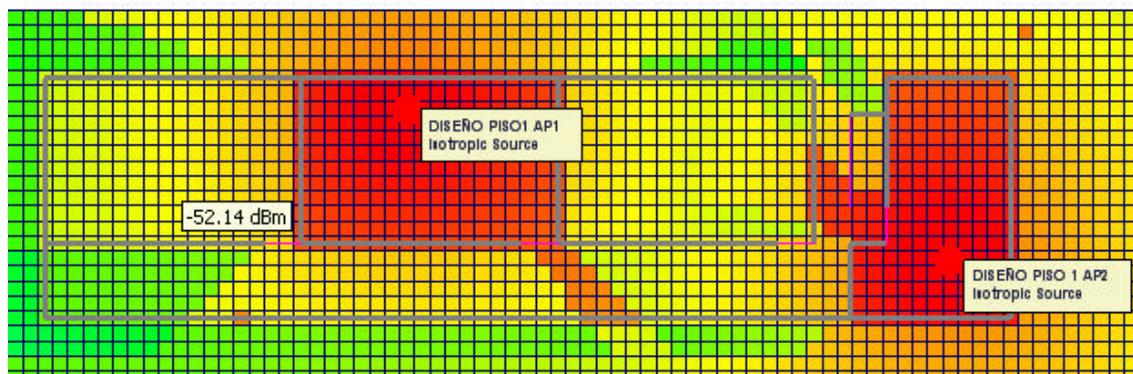
Ubicación de Access Point y Plano en DISEÑO Planta Baja



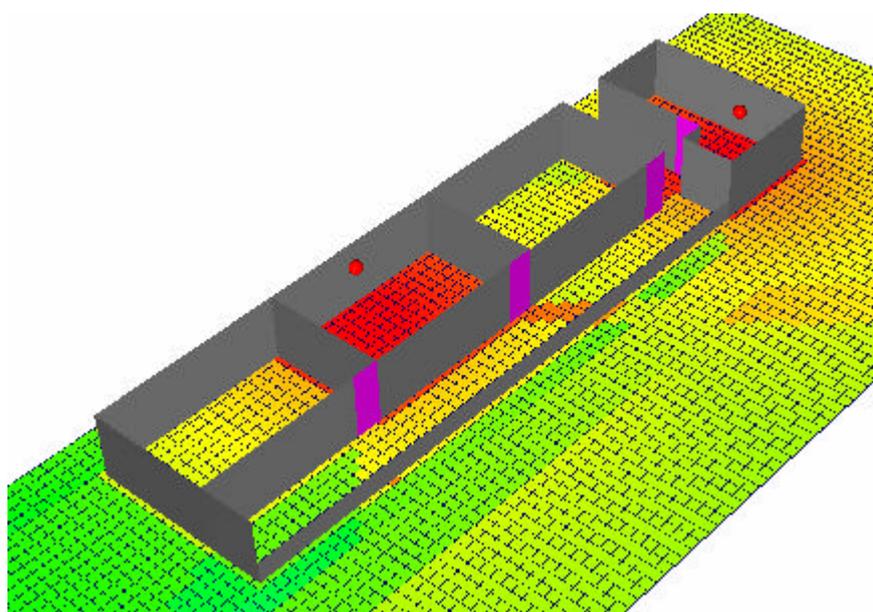
Propagación en 3D en DISEÑO Planta Baja

DISEÑO PISO 1

En esta planta se debe instalar dos access point como se observa para tener un buen nivel de campo y poder permitir el acceso



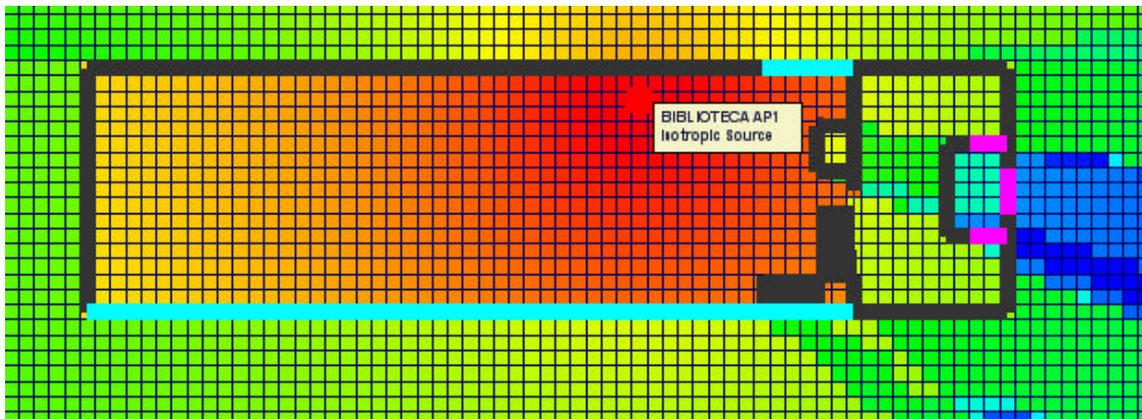
Ubicación de Access Point y Plano en DISEÑO Piso 1



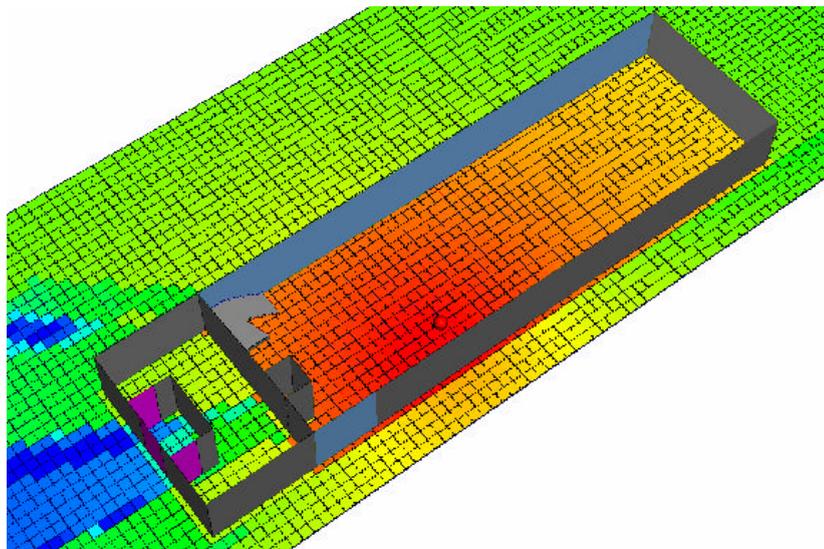
Propagación en 3D en DISEÑO Planta Baja

4.19.16 BIBLIOTECA.

En este lugar no se debe instalar access point ya que la cobertura y la capacidad del actual cumple con todos los requerimientos, ya que no existe mayor cantidad de paredes y obstáculos.



Ubicación de Access Point y Plano en la BIBLIOTECA



Propagación en 3D en la BIBLIOTECA

Como se observa en los gráficos de propagación de todos los sectores existe todavía lugares en donde por cobertura se debe aumentar los puntos de acceso es por esta razón que se debe tomar en cuenta el área exacta en donde se quiere brindar el servicio y la capacidad de los Access Point. No olvidar que para obtener todos estos gráficos de la propagación interior se tomo en cuenta las pérdidas generalizadas que se obtuvo en el calculo en el capítulo III y en el anexo 2.

CAPITULO V SEGURIDAD DE REDES WI-FI

5.1 Mecanismos de Seguridad

A continuación se realizará una breve descripción de los mecanismos de seguridad que existen para acceder a una red Wi-fi:

WEP (Wired Equivalent Privacy, Privacidad equivalente al Cable): Es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas versiones 802.11a, 802.11b y 802.11g. Emplea el algoritmo RC4 de RSA Data Security de 64 bits que es un sistema de clave compartida que utiliza los primeros 24 bits para el vector de inicialización y los 40 bits restantes para la clave secreta. El defecto de este sistema es que si se llega a capturar varias tramas de información con los diferentes vectores de inicialización se puede deducir la clave secreta.

Filtrado por MAC: Esto no es un sistema de protección en sí mismo si no que debe usarse como apoyo junto con otro de los sistemas mecanismos de seguridad. En teoría, cada tarjeta de red inalámbrica tiene una única dirección MAC que la identifica respecto al resto de tarjetas producidas. El filtrado funciona dejando acceso a la red sólo a las direcciones MAC seleccionadas por el usuario. Existen programas en muchas plataformas que permiten emular la MAC que se desee con lo cual se puede saltar esta seguridad.

WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi): Wap soluciona las vulnerabilidades encontradas en WEP implementa el Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande (48 bits), evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP. Además implementa una clave de 128 bits. Permite también utilizar una clave compartida (PSK o Pre-Shared Key), lo cual suple la complejidad de implementación de un servidor de autenticación

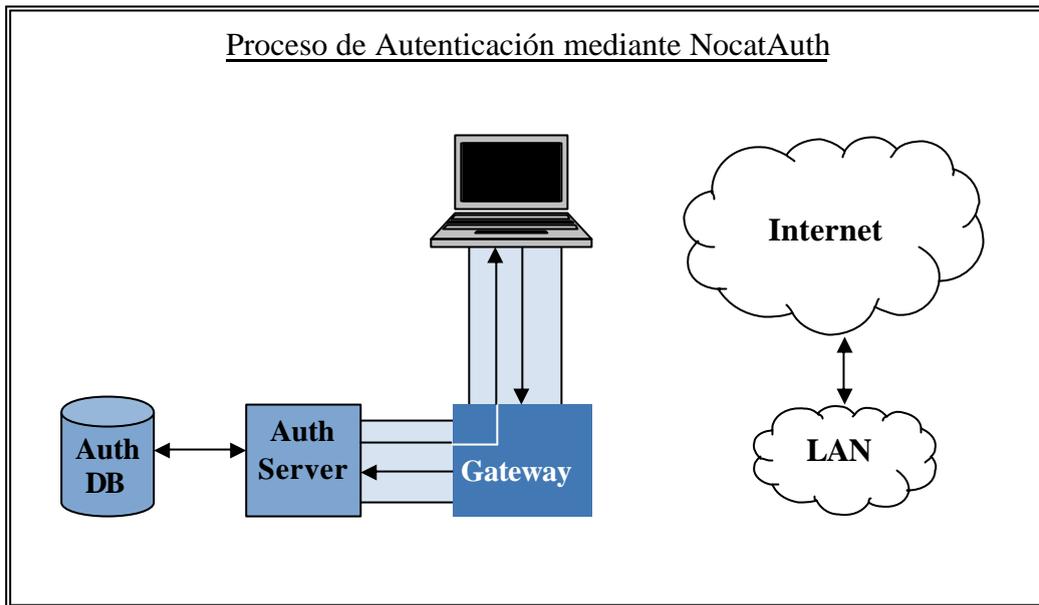
WPA implementa un código de integridad del mensaje (MIC - Message Integrity Code), también conocido como "Michael" y incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas. Para limitar el riesgo de ataques al código de integridad las redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

WPA2 No se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP (ver arriba). AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal.

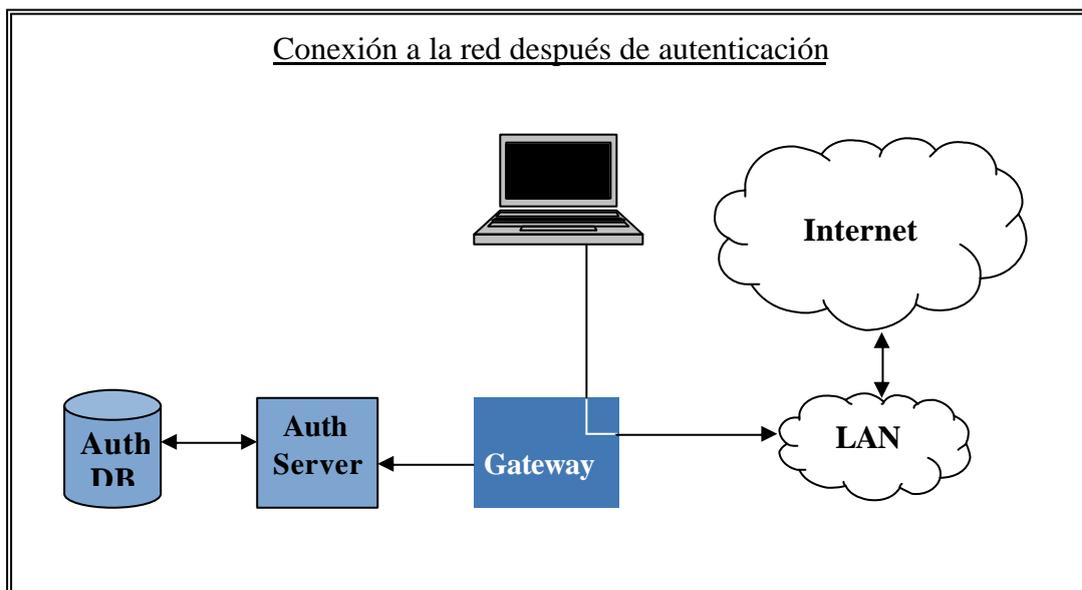
Portales Cautivos: Un portal cautivo es una página *web* en la que se presenta una solicitud de inicio de sesión al momento en que el usuario de una red pública y/o privada desea acceder a una conexión a Internet, garantizando así el uso normal y legal de la red. En caso que el usuario no inicie una sesión válida, no se le permite el tráfico de red a través de la puerta de enlace. Estos portales son utilizados principalmente por proveedores de *hot-spots* en aeropuertos, hoteles, cafeterías, cafés Internet, etc.

Al momento en que un usuario se autentica ante una red por primera vez, se presenta una página *Web* en la que se necesita de una serie de acciones antes de acceder como el aceptar las políticas de uso presionando un botón en la página. Un portal cautivo puede ser la puerta de acceso para conectar usuarios, redes u otros servicios. Las funciones principales que realiza un portal cautivo son:

1. Desplegar una página *Web* de inicio de sesión ante el usuario
2. Validar la identificación
3. Notificar a la puerta de enlace quién ingreso correctamente la identificación.
4. Administrar las conexiones locales
5. Gestionar el ancho de banda que se asignado a cada uno de los usuarios
6. Determinar las reglas del “*firewall*” o contrafuegos
7. Cerrar sesiones caducadas, antiguas o finalizadas
8. Utiliza SSL y PGP (*Prety Good Privacy* – Privacidad Bastante Buena) para la comunicación con la puerta de enlace y para las conexiones de los usuarios, esto hace que no se dependa de la seguridad WEP (Wired Equivalent Privacy), ni WPA (Wireless Protected Access – Acceso Protegido a Redes Inalámbricas).



Proceso de Autenticación mediante Nocat Auth



Conexión a la red después de la autenticación

La comunicación entre el portal cautivo y la puerta de enlace se realiza mediante mensajes firmados PGP mediante el sistema de autenticación, con lo que se reduce la posibilidad de que un usuario altere las reglas del “*firewall*” cortafuegos

Existen varios productos de *software* que permiten controlar el acceso de usuarios a los servicios de una red. Los dos más conocidos son: Nocat Auth y Chillispot

5.2 Mecanismo de Seguridad Escogido para la Red de La Universidad del Azuay

Debido a que a la red de La Universidad del Azuay pueden tener acceso entre estudiantes, empleados, trabajadores y profesores alrededor de 4500 personas se debía escoger un sistema de acceso de fácil distribución y sencillo de configurar en los equipos con los cuales se accede. Por esta razón la herramienta más cómoda a utilizar y analizando los casos en otras universidades como La Universidad de Extremadura (España), Universidad de Veracruz (México), Universidad de Zaragoza (España), Universidad de Córdoba (España), etc. Es la de Portales cautivos dentro de las herramientas de portales cautivos sobresale dos software libre Nocat y Chillispot.

Debido a que en el momento de hacer las evaluaciones el software Nocat era muy superior al de Chillispot y con las experiencias obtenidas en otras universidades se optó por el paquete Nocat.

5.3 Notac Auth

NoCat Auth es un programa escrito en los lenguajes de programación Perl y C, es el encargado de implementar el portal, solicitando al usuario que inicie una sesión mediante la presentación de una página *Web*, posteriormente valida esta identificación y en caso de ser correcta notifica a la puerta de enlace. Además gestiona el ancho de banda asignado a cada uno de los clientes y administra las conexiones. NoCat Auth, puede funcionar en tres modos: *Public*, *Member* y *Owner*.



El proceso de autenticación en NoCat Auth es:

1. El cliente se conecta a la red mediante la configuración TCP/IP, asignándole una IP, puerta de enlace, DNS, etc.
2. Se bloquea el acceso a cualquier lugar más allá del sistema de autenticación, esto se lo realiza de forma predeterminada.
3. El usuario realiza una petición *Web*.
4. A continuación se le redirige al servicio de puerta de enlace.
5. Nuevamente el usuario es redirigido al sistema de autenticación
6. Se le presenta los tres tipos de modos de autenticación, *Member*, *Public* y *Owner*.
7. En caso que las credenciales sean válidas, se crea un mensaje saliente firmado mediante PGP y se envía nuevamente hacia la puerta de enlace, este proceso se da entre el *gateway*, el sistema de autenticación y el portal cautivo.
8. La puerta de enlace mediante una clave pública proporcionada por el servicio de autenticación, comprueba y verifica la autenticidad del mensaje.
9. Si todo es correcto se modifican las reglas del cortafuegos y se redirige al usuario a la página que deseaba en el punto 3.

Para mantener activa y abierta la conexión, se abre un *pop-up* (JavaScript) al cliente que actualiza cada cierto tiempo el inicio de sesión, es por este motivo que se pueden anular sesiones antiguas o establecer límites de tiempo a las sesiones. En caso que el usuario cierre el *pop-up* o navegador requerirá realizar nuevamente todo el proceso de autenticación.

La autenticación puede ser configurada para realizarse contra un repositorio de datos, pudiendo ser este de varios tipos un archivo propio (MD5), una Base de Datos (MySQL o Postgres), LDAP (*Lightweight Directory Access Protocol*), Radius, PAM (*Pluggable Authentication Module*), Samba, IMAP (*Internet Message Access Protocol*)

El sistema que se escogió por comodidad es autenticación mediante la base de datos mysql, a futuro cuando el sistema este más estable se cambiará a un sistema de autenticación mediante un servidor Radius.

5.4 Instalación y Configuración de Nocath Auth

Para la instalación y configuración del servidor de autenticación se utilizo un servidor Pentium IV de 2.53 Ghz. con 1Gb de RAM y 200 Gb de Disco Duro con 2 tarjetas de Red Ethernet. Este equipo servirá como puerta de enlace hacia Internet.

El Software que se necesitará para la implementación del sistema es:

LINUX con kernel 2.4.x con Iptables Centos 4.0:

Servidor Apache 2.0 + mod_ssl

- ◆ Perl versión 5.6 o superior con los módulos:
- ◆ Net::Netmask
- ◆ Digest::MD5
- ◆ GnuPG
- ◆ Un servidor DHCP
- ◆ Un Servidor DNS
- ◆ MySQL

5.4.1 Instalación del Software Nocat

Una vez instalados todos los requisitos de software, se procede a realizar la instalación del servidor de autenticación. Los pasos para la instalación del servidor NoCat Auth se detalla a continuación.

- a) Se descarga el archivo de instalación de la página de NoCat <http://nocat.net/download/NoCatAuth/NoCatAuth-0.82.tar.gz>
- b) Se descomprime el archivo NoCatAuth-0.82.tar.gz


```
# tar zxvf NoCatAuth-0.82.tar.gz
```
- c) Se accede al directorio de compilación


```
# cd NoCatAuth-0.82
```
- d) Se crea el directorio donde se instalarán los archivos de NoCat


```
# mkdir /usr/local/nocat
```
- e) Se instala el *Gateway* NoCat indicando la ruta donde se creará el ejecutable.


```
# make PREFIX=/usr/local/nocat/gateway gateway
```

Si estamos trabajando con una versión de kernel mayor a la 2.4.x como es nuestro caso que estamos trabajando con una versión 2.6 se desplegará en pantalla un error debido a la incompatibilidad con los iptables del kernel, ya que los archivos de instalación de NoCat fueron diseñados para trabajar con versión 2.4.x. La solución a este problema es modificar en el directorio NoCatAuth-0.82/bin/ el archivo detect-fw.sh la línea que dice Linux 2.4 por Linux 2.6., y volver a ejecutar la línea anterior.

- f) Se crea el servidor de autenticación indicando la ruta donde se instalará el servidor de autenticación NoCat.


```
# make PREFIX=/usr/local/nocat authserv
```

- g) Se crean las llaves y certificados que utilizará NoCat para su funcionamiento.

```
# make PREFIX=/usr/local/nocat pgpkey
```

La ejecución de esta línea llevará a una serie de preguntas; se puede responder con las respuestas que se indican por defecto.

- h) En las últimas líneas de compilación del paso anterior se indica que se ha instalado la clave pública en el archivo `usr/local/nocat/trustedkeyd.gpg`. Este archivo se lo debe copiar al directorio de las llaves públicas del *gateway*.

```
# cp /usr/local/nocat/trustedkeys.gpg
  /usr/local/nocat/gateway/pgp
```

- i) Se dan permisos de lectura para el usuario con el que corre apache al directorio de las llaves públicas del *gateway*.

```
# chown -R apache:apache /usr/local/nocat/pgp
```

- j) Se copian los archivos `authserv.conf` y `gateway.conf` desde el directorio `NoCatAuth-0.82`

```
# cp authserv.conf /usr/local/nocat/nocat.conf
# cp gateway.conf /usr/local/nocat/gateway/nocat.conf
```

Estos dos archivos llevan el mismo nombre pero cumplirán funciones diferentes. El primero servirá para la configuración del portal y el segundo para la configuración del *gateway*.

- k) Se copia el archivo `authserv.conf` desde el directorio `NoCatAuth-0.82/etc/`

```
# cp etc/authserv.conf /usr/local/nocat/etc/
```

Este archivo nos servirá para la configuración del SSL del Apache, más adelante se explicará su uso.

Básicamente para la configuración de NoCat se realizó la modificación de algunas líneas en los archivos `/usr/local/nocat/nocat.conf`, `/usr/local/nocat/gateway/nocat.conf`, y `/etc/httpd/conf.d/ssl.conf` adecuándolos a las características de nuestros componentes y a nuestras necesidades.

5.4.2 Configuración del portal `/usr/local/nocat/nocat.conf`

Las líneas que debe tener este archivo son las siguientes:

- a) El directorio donde se encuentran almacenadas las llaves PGP.

```
PGPKeyPath /usr/local/nocat/pgp
```

- b) El directorio donde se encuentran alojadas las páginas que utilizará NoCat.

DocumentRoot /usr/local/nocat/htdocs

- c) El método de autenticación a utilizarse pudiendo ser este: DBI, Passwd, LDAP, RADIUS, PAM, Samba, IMAP.

DataSource DBI

- d) Configuración del modo de autenticación utilizado en nuestro caso a través de Base de Datos MySQL (DBI).

Database dbi:mysql:database=nocat

DB_User nocat

DB_Passwd nocatauth

- e) Configuración de las tablas y campos de la base datos a utilizar.

UserTable member

UserIDField login

UserPasswdField pass

UserAuthField status

UserStampField created

GroupTable network

GroupIDField network

GroupAdminField admin

- f) El largo mínimo de caracteres para el *password*.

MinPasswdLength 6

- g) La dirección IP de nuestro *gateway* (interfaz interna) así como la de la red a la que pertenece.

LocalGateway 192.168.10.1

LocalNetWork 192.168.10.0

- h) Las páginas que utilizará el servidor para realizar todo el trabajo de autenticación, registro, etc

LoginForm login.html

LoginOKForm login_ok.html

FatalForm fatal.html

ExpiredForm expired.html

RenewForm renew.html

PassiveRenewForm renew_pasv.html

RegisterForm	register.html
RegisterOKForm	register_ok.html
RegisterFields	name url description
UpdateForm	update.html
UpdateFields	url description

i) Los diferentes mensajes que se presentarán al usuario.

LoginGreeting	Bienvenido a la Red.		
LoginMissing	Por favor, complete todos los campos		
LoginBadUser	El usuario no parece correcto,	inténtelo de	nuevo
LoginBadPass	El usuario y clave escritos no	concuerdan,	escriba nuevamente.
LoginBadStatus	Lo sentimos, no esta registrado en	la Red	
RegisterGreeting	Bienvenido!, Introduzca los datos	correspondientes para poder	registrarlo.
RegisterMissing	Nombre, Usuario, y password son	obligatorios	
RegisterUserExists	Usuario ya esta registrado.		
RegisterBadUser	El usuario no esta correcto, repita	nuevamente	
RegisterInvalidPass	La contraseña debe ser de 6	caracteres	como mínimo.
RegisterPassNoMatch	Las contraseña suministradas	no	concuerdan, repita.
RegisterSuccess	Su registro ha sido completado satisfactoriamente		
UpdateGreeting	Introduzca e-mail y contraseña		
UpdateBadUser	El mail no parece correcto, repita	nuevamente	
UpdateBadPass	El mail y password escritos no	concuerdan,	repita nuevamente.
UpdateInvalidPass	La contraseña debe ser de 6	caracteres	como mínimo.
UpdatePassNoMatch	El mail y password escritos no	concuerdan,	repita nuevamente.
UpdateSuccess	Enhorabuena, su registro se ha	completado	satisfactoriamente.

5.4.3 Configuración del Gateway /usr/local/nocat/gateway/nocat.conf

Las líneas que debe tener este archivo son:

a) El nombre del *gateway* que se presenta en el *splash* y las páginas.

GatewayName Servidor de Autenticación NoCat

b) El modo de operación del *Gateway*. Como se explicó en el Capitulo 3 puede ser: *Captive*, *Passive*, *Open*. Utilizamos el modo *Captive*.

GatewayMode *Captive*

- c) El archivo .log que nos permitirá controlar todo lo que sucedió en el servidor.

GatewayLog /usr/local/nocat/nocat.log

- d) El tiempo en Segundos que se le permitirá a un cliente permanecer conectado. Este tiempo puede ser configurado dependiendo de las necesidades.

LoginTimeout 86400

- e) El directorio donde se encuentran alojadas las páginas que utilizará NoCat.

DocumentRoot /usr/local/nocat/gateway/htdocs

- f) El *splash* de captura del usuario.

SplashForm splash.html

- g) El *splash* de estado de conexión que deberá permanecer abierto durante la navegación

StatusForm status.html

- h) La dirección IP del servidor de autenticación

AuthServiceAddr 192.168.10.1

- i) El URL al que será redireccionado el cliente cuando intente acceder al Internet antes de autenticarse.

AuthServiceURL https://\$AuthServiceAddr/cgi-bin/login

- j) El URL al que se redireccionará al cliente después de haber culminado su tiempo de conexión.

LogoutURL https://\$AuthServiceAddr/logout.html

- k) La configuración de las interfaces interna (por donde acceden los clientes) y externa (salida al Internet).

ExternalDevice eth0

InternalDevice eth1

El nombre de las interfaces pueden variar y se debe tener muy en cuenta cuál es cual interfaz ya que si se especifican mal los nombres podrían existir muchos problemas.

- l) La dirección IP de la red Interna.

LocalNetwork 192.168.10.0/24

- m) Los puertos TCP a los que se les excluirá el acceso cuando alguien inicie una sesión como un usuario de clase pública.

ExcludePorts 25

- n) El directorio donde se encuentran almacenadas las llaves PGP.

```
PGPKeyPath /usr/local/nocat/pgp
```

5.4.4 Configuración del archivo /etc/httpd/conf.d/ssl.conf

Lo único que se debe hacer con este archivo es incluir en su contenido la ruta del archivo authserv.conf. La línea que se debe agregar es:

```
Include /usr/local/nocat/etc/authserv.conf
```

El archivo authserv.conf fue anteriormente copiado de las fuentes del NoCat y lo que hace es indicar a Apache la ruta del alias /cgi-bin/ para que busque en el directorio donde se encuentran los archivos Perl del NoCat y la configuración de ese directorio. Las líneas de este archivo son:

```
ScriptAlias /cgi-bin/ /usr/local/nocat/cgi-bin/
<Directory /usr/local/nocat/cgi-bin>
    SetEnv PERL5LIB /usr/local/nocat/lib
    SetEnv NOCAT /usr/local/nocat/nocat.conf
</Directory>
```

5.4.5 Configuración de las Interfaces

Las interfaces que tiene nuestro sistema de autenticación son 2: la interfaz interna (eth1) que es por donde acceden los usuarios al *gateway*, y la interfaz externa (eth0) que es por donde salen al Internet. Asignamos las direcciones IP, máscara y *gateway* a las dos interfaces. Es conveniente de que cada interfaz pertenezcan a redes diferentes.

	eth0	eth1
Dirección IP	192.188.47.5	192.168.10.1
Máscara de Subred	255.255.255.0	255.255.255.0
Gateway	192.188.47.5	

Además de lo anterior se debe especificar la dirección del DNS que utilizara el servidor.

DNS primario: 127.0.0.1

DNS secundario:192.188.47.2

5.4.6 Configuración del cliente

Lo que hay que configurar en el equipo cliente es que la dirección IP, *gateway* y DNS sea asignada desde el servidor mediante DHCP. Y para conectarse al Internet configurar el *browser* para que no utilice ningún Proxy, sino que se conecte directamente.

5.4.7 Creación de la base de datos de los usuarios

Los usuarios estarán registrados en una base de datos MySQL. La base datos como se mostraba en los archivos de configuración tendrá el nombre nocat.

Primeramente iniciamos la base de datos MySQL

```
# /etc/init.d/mysqld start
```

Creamos la base de datos nocat y digitamos una contraseña (la que está en el archivo de configuración es 'nocatauth'). La contraseña puede ser otra, pero se tendría también que cambiar tanto el archivo de configuración como en algunos de los programas Perl que acceden a la base de datos debido a que 'nocatauth' es la que viene por defecto.

```
# mysqladmin create nocat -p
Enter password:
```

Una vez creada la base de datos se procede a la creación de las tablas. Para facilitarnos el trabajo de crear las tablas, Nocat cuenta con un *script* que contiene las rutinas para realizar dicha tarea. Este *script* está en NoCatAuth-0.82/etc/nocat.schema; entonces añadimos la estructura a la base de datos nocat.

```
# mysql nocat < nocat.schema -p
```

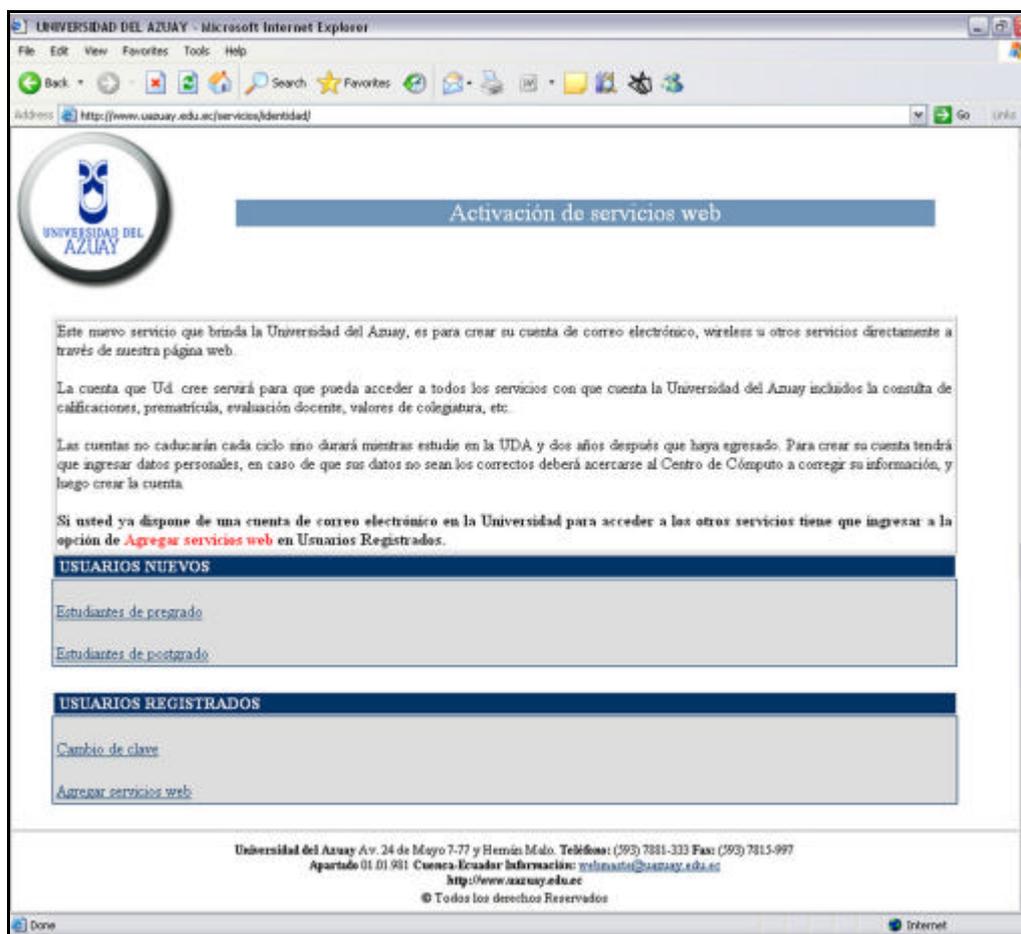
Asignamos todos los privilegios de *root* de todas las tablas de la base de datos nocat al usuario nocat.

```
# mysql -u root -pcontrasena
mysql> grant all on nocat.* to nocat@localhost identified
by 'nocatauth';
mysql> flush privileges;
```

5.4.8 Creación de Usuarios Para Nocat

El sistema de creación de usuarios que tiene nocat es un sistema mediante comandos de consola por lo que no es conveniente para la utilización en un entorno público por lo que se creo una aplicación automática de creación de cuentas con lo cual los estudiantes

ingresan algunos datos personales para validar su identidad y obtener la clave de acceso a la red wireless de la Universidad del Azuay.



El sistema identifica a los usuarios nuevos como los estudiantes de pregrado o de postgrado que no tengan una cuenta para el correo electrónico de la Universidad del Azuay

Para que el estudiante pueda crearse una cuenta para los servicios Web de la Universidad del Azuay, primero deberá llenar un formulario con datos personales que verifiquen que el estudiante es quien dice ser, estos datos son los siguientes:

Si es un estudiante de pregrado:

- ◆ Nombres
- ◆ Apellidos
- ◆ Código de estudiante
- ◆ Cédula de Identidad o Pasaporte.
- ◆ Teléfono
- ◆ Sexo
- ◆ Libreta Militar (si es varón y mayor de 18 años)
- ◆ Tipo de Sangre
- ◆ Estado civil

- ◆ Colegio
- ◆ Carrera

Si es un estudiante de postgrado:

- ◆ Nombres
- ◆ Apellidos
- ◆ Cédula de Identidad
- ◆ Teléfono
- ◆ Sexo
- ◆ Libreta Militar (si es varón y mayor de 18 años)
- ◆ Tipo de Sangre
- ◆ Estado civil
- ◆ Carrera
- ◆ Lugar de Trabajo

A los estudiantes se les presentará el siguiente formulario, cabe recalcar que todos los datos son requeridos por el sistema:

Si es un estudiante de postgrado:

The screenshot shows a web browser window with the title 'INGRESO DE DATOS - Microsoft Internet Explorer'. The address bar shows the URL: http://www.uazuay.edu.ec/servicios/identidad/datos_maestria.php. The page content includes the University of Azuay logo and a header 'NUEVA CUENTA DE USUARIO'. Below this is a section titled 'Ingreso sus Datos Personales' with the following fields:

- Cédula o Pasaporte (Sin guión): 0181267409
- Nombres: Pablo Xavier (Los nombres no deben contener tildes o acentos)
- Apellidos: Marquez Cordero (Los apellidos no deben contener tildes o acentos)
- Teléfono: 259160
- Sexo: masculino
- Libreta Militar: 15730109887 Sin Libreta
- Fecha de Nacimiento: 9 Enero 1973
- Tipo de Sangre: OPH+
- Estado Civil: SOLTERO(A)
- Lugar de Trabajo: CRAVATTE
- Carrera: MAESTRIA ADMIN DE EMPRESAS - MBA

At the bottom, there is a section for a verification code: 'Escriba aquí el número que aparece a continuación'. The 'Número Verificador' is 1595505693, and the code shown in the image is 1595505693. There are 'VALIDAR' and 'BORRAR' buttons at the bottom left.

Ingreso de datos personales del estudiante de postgrado en el sistema

Para verificar que los datos sean correctos el sistema debe conectarse a las bases de datos del sistema académico de la Universidad del Azuay que contienen la información de los estudiantes.

Este Sistema fue desarrollado en los lenguajes de programación Web HTML, PHP

Si es un estudiante de pregrado:

The screenshot shows a web browser window titled 'INGRESO DE DATOS - Microsoft Internet Explorer'. The address bar shows 'http://www.azuay.edu.ec/servicios/identidad/datos_usuario.php'. The page content includes the Universidad del Azuay logo and a blue header with the text 'NUEVA CUENTA DE USUARIO'. Below this is a section titled 'Ingrese sus Datos Personales' with the following fields:

- Código: 24833
- Nombre: Diego Xavier (Los nombres no deben contener tildes o acentos)
- Apellidos: Rojas Pizarro (Los apellidos no deben contener tildes o acentos)
- Cédula o Pasaporte (Sin guión): 0183789781
- Sexo: masculino
- Libreta Militar: 01000283, Sin Libreta
- Fecha de Nacimiento: 8 Febrero 1983
- Tipo de Sangre: O+
- Estado Civil: Soltero
- Carrera: CURSO GRADUACIONING SISTEMAS - CIS
- Número Verificador: 1875417521, 1879417521

At the bottom of the form are 'VALIDAR' and 'BORRAR' buttons. The footer of the page contains contact information for the Universidad del Azuay.

5.4.9 Iniciando el servidor de Nocat Auth

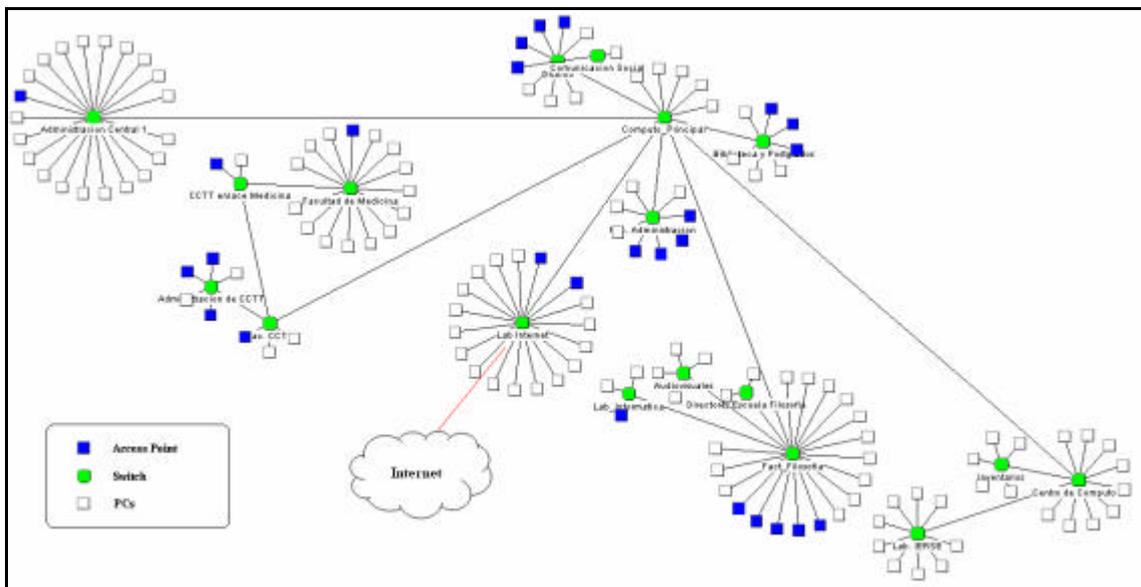
Para iniciar el servidor nocat previamente hay que iniciar otros servicios:

- ◆ Para iniciar iptables se ejecuta `service iptables start`
- ◆ Para iniciar el servidor de dhcp se ejecuta `service dhcpd start`
- ◆ Para iniciar el servidor de DNS se ejecuta `service bind start`
- ◆ Para iniciar nocat se ejecuta el comando `/usr/local/nocat/gateway/bin/gateway start`

6. Seguridad en la Red

La Red Wireless de la Universidad del Azuay se comunica hacia el Internet a través de la Red Lan de la misma por lo cual cualquiera que se pueda conectar a la red Wlan podría atacar a cualquier pc de la red Lan incluido los servidor por esta razón se tubo que crear una red vlan para la red Wlan de esta forma se evita el acceso a la red Lan.

La Red Lan de la Universidad del Azuay cuenta con switchs 3com 4228G y 4226T repartidos en el campus tal como lo indica el siguiente esquema de red:



6.1 Configuración de Vlan

La configuración de la Vlan en los Switch no se puede realizar por medio del entorno Web de configuración que tiene el Switch por lo que se lo debe realizar mediante la consola de comandos del mismo:

- 1.- Se ingresa al Switch 3com mediante telnet hacia la IP del switch.
- 2.- En el menú que muestra el switch cuando se ingresa se sigue las siguientes opciones para la creación de la Vlan

Bridge

Vlan

Create(Se crean las Vlan)

- Numero de Vlan Ejemplo (AL1,1:24)
- Nombre de la Vlan

Delete(Borrar vlan)

- Número de Vlan a borrar

Detail (Detalla que puertos están en cada vlan)

- Numero de Vlan a visualizar o all(todas)

Modify (Modificar).

- Addport (Añadir un puerto a la Vlan)
- Name
- Remove Port (borrar puerto)

Se muestra la configuración del switch de la Facultad de Administración:

Select VLAN ID (1-2,all)[all]: all

VLAN ID: 1 Name: Default VLAN

Unit	Untagged Member Ports	Tagged Member Ports
1	1-19,26-28	none
2	1-25,27-28	none
Aggregated Links	AL1,AL3-AL4	none

VLAN ID: 2 Name: Wireless

Unit	Untagged Member Ports	Tagged Member Ports
1	20-24	27
2	none	none
Aggregated Links	AL2	none

Tagged = puerto de comunicarnos entre switches

Untagged = puertos de cada Vlan en el switches

Nota: El puerto tagged debe estar en la ultima posición de las vlan que se desea conectar.

CONCLUSIONES

Luego del cálculo realizado con el modelo de propagación Log-normal shadowing path loss y obtener la N generalizada, se puede utilizar cualquier herramienta de simulación para proyectar los nuevos puntos de la Red Wlan sin necesidad de tomar medidas de campo.

En todos los pisos de las diferentes facultades a excepción de la biblioteca y la planta baja de administración se necesitan reubicar y adicionar un Access Point para cubrir todo el piso con una calidad de conexión de 54 Mbps

El costo de las herramientas de simulación de propagación son muy elevados y difíciles de conseguir a excepción de la herramienta utilizada RPS que es la única que proporciona una versión para estudiante totalmente gratis y permite incluir nuevos modelos de propagación.

La utilización de software libre (Nocat) para la autenticación a la red Wlan de la Universidad del Azuay permitió poder acoplar el sistema de autenticación de la red Wlan con los otros sistemas de autenticación con que cuenta La Universidad del Azuay ya que se pudo modificar su código sin ningún inconveniente

La seguridad mediante WPA, WEP o Filtrado de MAC en entornos públicos no es viable debido a la necesidad de repartir llaves y configurar PC manualmente para que estés se puedan conectar a la Wlan.

RECOMENDACIONES

Comprar un certificado digital para el sistema de autenticación ya que el que se está utilizando actualmente es generado con el servidor apache y cuando se ingresa con el Internet Explorer muestra una advertencia indicando que el ingreso al sitio Web no es recomendado.

Comprar el programa RPS para realizar un análisis completo del campus universitario y no solo por edificio.

No utilizar la red WLAN para acceso a sistemas internos propios de La Universidad ya que esta es una red pública por la cual se transmiten datos sin cifrar.

BIBLIOGRAFÍA

- ◆ <http://wifiepcc.unex.es/> Proyecto Extremadura Wireless 2006–Junio-01
- ◆ <http://www.anuies-noroeste.uson.mx/rscn/reuniones/06/materiales.htm> Autenticación para Redes Inalámbricas a través de software libre 2006-Mayo-25
- ◆ <http://www.rediris.es/cert/doc/reuniones/fs2006/archivo.es.html> Mesa Redonda “Desplegando Wlan: Bueno, Bonito y ... Seguro? ”, José Antonio Valero, Universidad de Zaragoza 2006-Enero-23
- ◆ <http://www.uco.es/servicios/informatica/index.php?go=comunicaciones/wireless/nocat.html&menu=17> Universidad de Córdoba, España, Servicios de Informática de la Universidad de Córdoba 2006-Agosto-15
- ◆ http://www.utpl.edu.ec/eccbog/wp-content/uploads/2007/04/redes_diseno-e-implementacion-del-modulo-de-seguridad-para-la-red-wireless-de-la-utpl.doc Universidad Técnica Particular de Loja, Diseño e implementación del módulo de seguridad para la red Wireless de la UTPL 2007-Enero-15
- ◆ <http://nocat.net/> Portal Cautivo Nocat, 2005-Diciembre-12
- ◆ Sistema de Autenticación unificado para la utilización de los servicios Web de los estudiantes de La Universidad del Azuay, Rojas Diego, Marzo 2007
- ◆ Instalación y Configuración de un servidor de autenticación vía portal cautivo mediante el sistema nocat Auth sobre Linux, Barros María Paula, Cobos Joseph, Febrero 2006
- ◆ <http://www.chillispot.org/> Portal Cautivo Chillispot , 2005-Diciembre-12
- ◆ <http://blyx.com/public/wireless/nocatbox/nocatbox-howto-es.pdf>, DIAZ, Toni. NoCatBox HOWTO v1.4 . 2005-Diciembre-12.
- ◆ <http://www.php.net/manual/en/index.php> Php group, funciones de php, 2007-Enero-08
- ◆ <http://dev.mysql.com/doc/> Mysql AB, funciones de Mysql, 2006-October-15
- ◆ <http://perlenespanol.baboonsoftware.com/tutoriales/> Perl En Español, funciones de Perl 2006-Julio-20
- ◆ http://www.zend.com/products/zend_core/zend_core_for_oracle Zend, Descarga, instalación y configuración del Zend Core para Oracle, citado 2007-Enero-15
- ◆ <http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf> Modelo de Cobertura en Redes Inalámbricas basada en Radiosidad por Refinamiento Progresivo. Tesis de Doctorado en la universidad de Cataluña. Autor: Nestor Garcia Fernandez Marzo / 2006
- ◆ AWFSS v.4 Aironet Wíreles LAN. Fundamentals and CISCO AIRONET. Wireless Site Survey.
- ◆ “Optimization of Wireless Communication Systems Using Cross-Layer Information”, L. Alonso and R. Agustí, ACM Signal Processing, vol.86, issue 8, pp. 1755-1772, August 2006.
- ◆ “The handbook of Ad Hoc Wireless Networks”, Mohammad Ilyas ,CRC Press, 2003.
- ◆ “Transmisión por Radio”, J. M. Hernando, Editorial Universitaria Ramón Areces, 2006.
- ◆ <http://www.educando.edu.do/NR/rdonlyres/330C83A3-1C8E-4AC2-B077801DB93A6E7/0/WIFI.pdf> ,Teoría de redes inalámbricas ,marzo/ 2007
- ◆ <http://ieeexplore.ieee.org/book/0470848871.01.pdf> Recomendaciones de la IEEE, enero 2007
- ◆ <http://upload.wikimedia.org/wikipedia/pl/6/69/Roaming.jpg>

GLOSARIO

GPRS (General Packet Radio Service): Estándar de comunicaciones móviles que permite velocidades de hasta 115 Kbps.

GSM (Global System for Mobile Communications): Sistema global de comunicaciones móviles de segunda generación (2G) que permite comunicaciones de hasta 9,6 Kbps.

IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones del IEEE

IMAP (Internet Message Access Protocol) IMAP (acrónimo inglés de Internet Message Access Protocol) es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP.

Iptables Los Iptables son una herramienta que nos permite configurar las reglas del sistema de filtrado (firewall) de paquetes del kernel de Linux, se ha desarrollado aun más a partir del kernel 2.4.

LDAP (Lightweight Directory Access Protocol) Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos (aunque su Sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.

Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados...).

MAC Media Access Control address

Mysql Es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones¹. MySQL AB desarrolla MySQL como software libre en un esquema de licenciamiento dual. Por un lado lo ofrece bajo la GNU GPL, pero, empresas que quieran incorporarlo en productos privativos pueden comprar a la empresa una licencia que les permita ese uso. Está desarrollado en su mayor parte en ANSI C.

PAM (Pluggable Authentication Module) El módulo de autenticación enchufable (PAM - Pluggable Authentication Module) es un marco de autenticación estándar del sector. El PAM aporta a los administradores de sistema flexibilidad para elegir cualquier servicio de autenticación disponible en el sistema a fin de llevar a cabo la autenticación. El marco PAM también permite enchufar y poner en funcionamiento módulos de servicio de autenticación nuevos sin modificar las aplicaciones.

PDA Personal digital Assistant Asistente Digital Personal

PHP (PHP Hypertext Pre-processor) Es un lenguaje de programación usado frecuentemente para la creación de contenido para sitios web con los cuales se puede programar las paginas html y los codigos de fuente. PHP es un acrónimo recursivo que significa "PHP Hypertext Pre-processor" (inicialmente PHP Tools, o, Personal Home Page Tools), y se trata de un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios web. Últimamente también para la creación de otro tipo de programas incluyendo aplicaciones con interfaz gráfica usando las librerías GTK+.

Radius (Remote Authentication Dial-In User Service) El servidor Radius es un servidor tipo AAA (Authentication, authorization, Accounting) Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

RPS (Radiowave Propagation Simulator) Herramienta para simulación de propagación.

Samba Es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con Linux o Mac OS X se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

UMTS (Universal Mobile Telecommunications System)

VLAN Acrónimo de Virtual LAN, 'red de área local virtual' es una red de computadoras lógicamente independiente. Varias VLANs pueden coexistir en un único switch físico.

WiMAX (Worldwide Interoperability for Microwave Access)

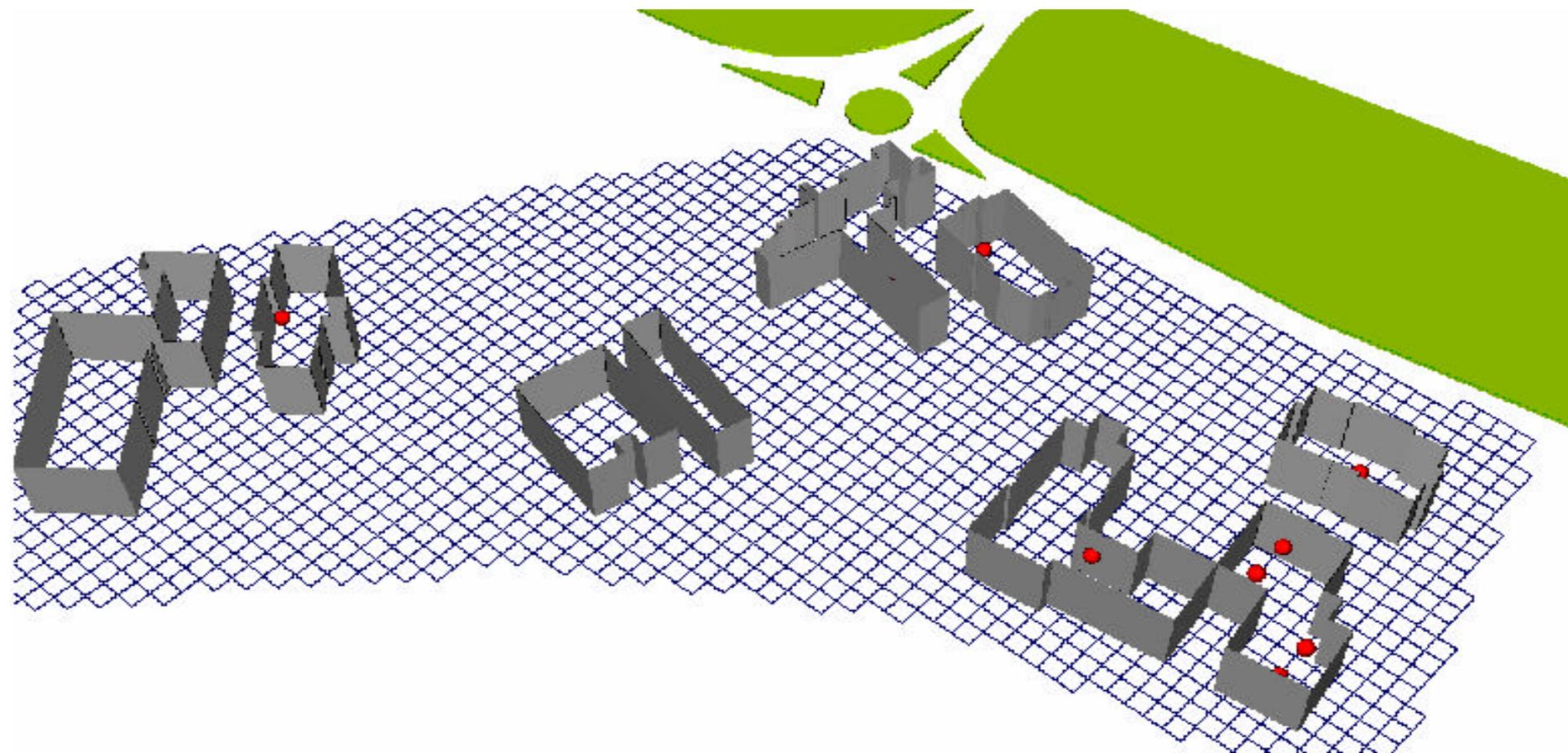
WI-FI Wireless Fidelity, Fidelidad Inalámbrica.

WLAN Redes Locales Inalámbricas.

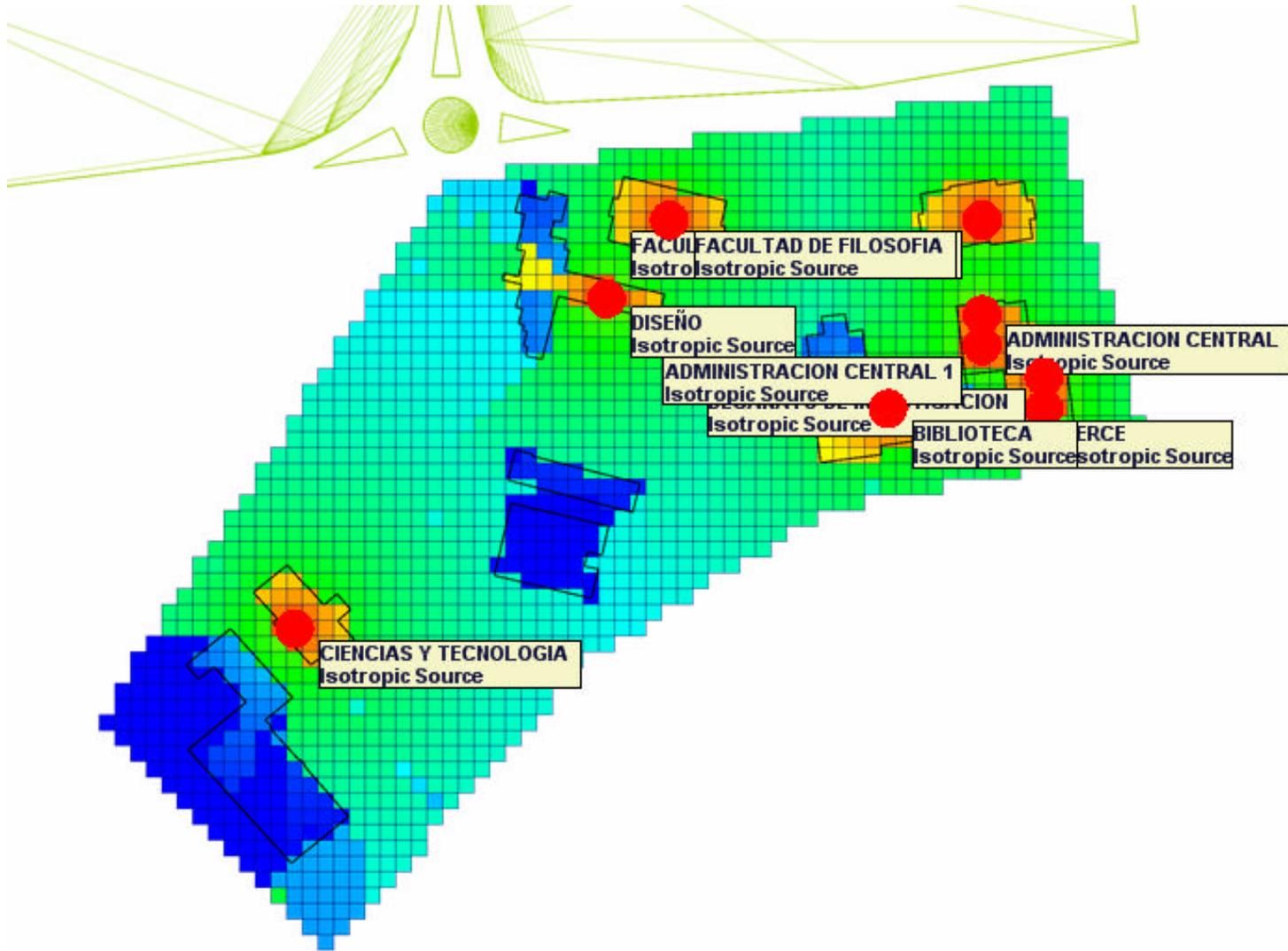
ANEXO 1
Croquis y ubicación de los Access Point



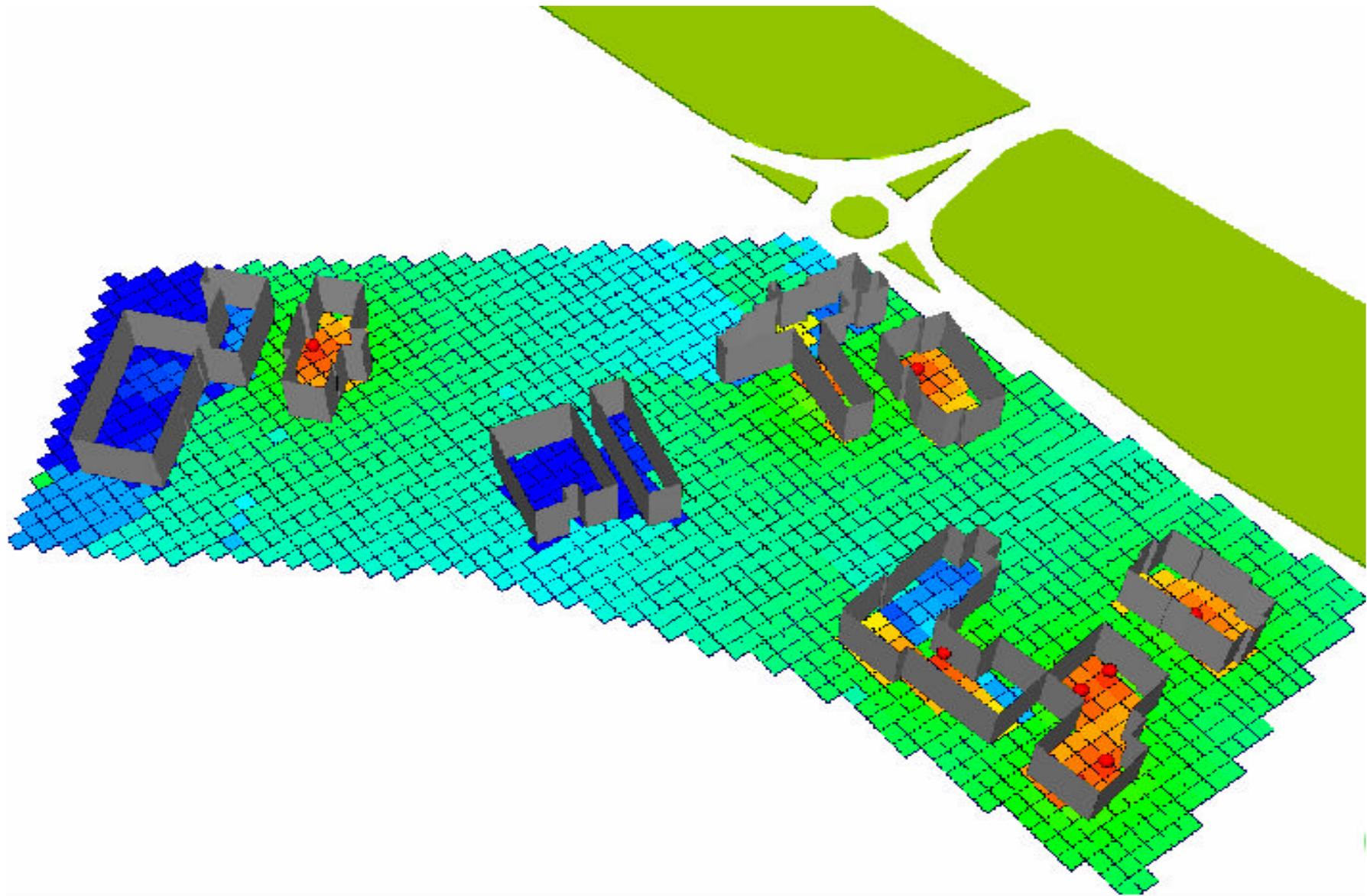
UBICACIÓN DE ACCESS POINT EN CAMPUS UNIVERSITARIO EN 2D



UBICACIÓN DE ACCESS POINT EN CAMPUS UNIVERSITARIO EN 3D



PROPAGACION EN CAMPUS UNIVERSITARIO EN 2D



PROPAGACION EN CAMPUS UNIVERSITARIO EN 3D

ANEXO 2

Tablas de Cálculos del modelo de propagación para cada Access Point

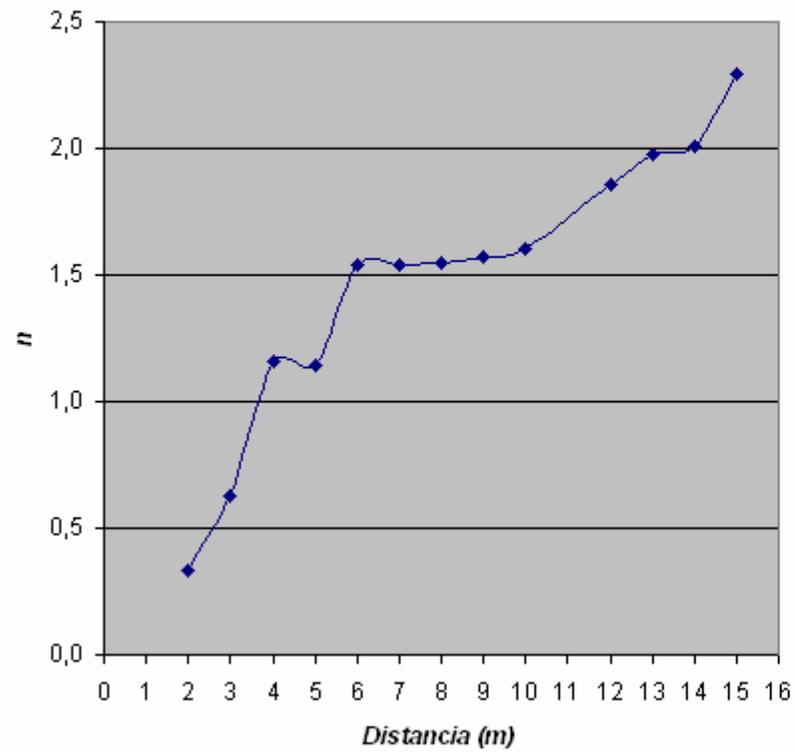
BIBLIOTECA

d0	PL(d0)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)	
1	-35	-36	2	n=	0,33219281	3,44631945	55,10527466	46,10991817	46,63794351	0,0000015184	-28,18600127
1	-35	-38	3	n=	0,62877098	4,04724960	58,02585660	49,63174335	46,95759530	0,0000006749	-31,70782645
1	-35	-42	4	n=	1,16267483	1,89263890	60,08457101	52,13051808	47,17092041	0,0000003796	-34,20660119
1	-35	-43	5	n=	1,14454125	2,32403406	61,67450650	54,06871834	47,32946075	0,0000002430	-36,14480145
1	-35	-47	6	n=	1,54211665	-0,50643095	62,96941530	55,65234326	47,45483455	0,0000001687	-37,72842637
1	-35	-48	7	n=	1,53828306	-0,51760320	64,06149254	56,99127906	47,55808404	0,0000001240	-39,06736216
1	-35	-49	8	n=	1,55023311	-0,66104164	65,00555074	58,15111800	47,64558069	0,0000000949	-40,22720110
1	-35	-50	9	n=	1,57192746	-0,90550080	65,83683253	59,17416844	47,72132164	0,0000000750	-41,25025155
1	-35	-51	10	n=	1,60000000	-1,22964649	66,57933797	60,08931826	47,78797277	0,0000000607	-42,16540136
1	-35	-55	12	n=	1,85325682	-4,06011150	67,86184694	61,67294318	47,90094674	0,0000000422	-43,74902628
1	-35	-57	13	n=	1,97496578	-5,54666290	68,42397988	62,36818530	47,94963108	0,0000000359	-44,44426841
1	-35	-58	14	n=	2,00675660	-6,07128375	68,94395225	63,01187897	47,99422430	0,0000000310	-45,08796207
1	-35	-62	15	n=	2,29574022	-9,62871635	69,42762737	63,61114344	48,03533202	0,0000000270	-45,68722654

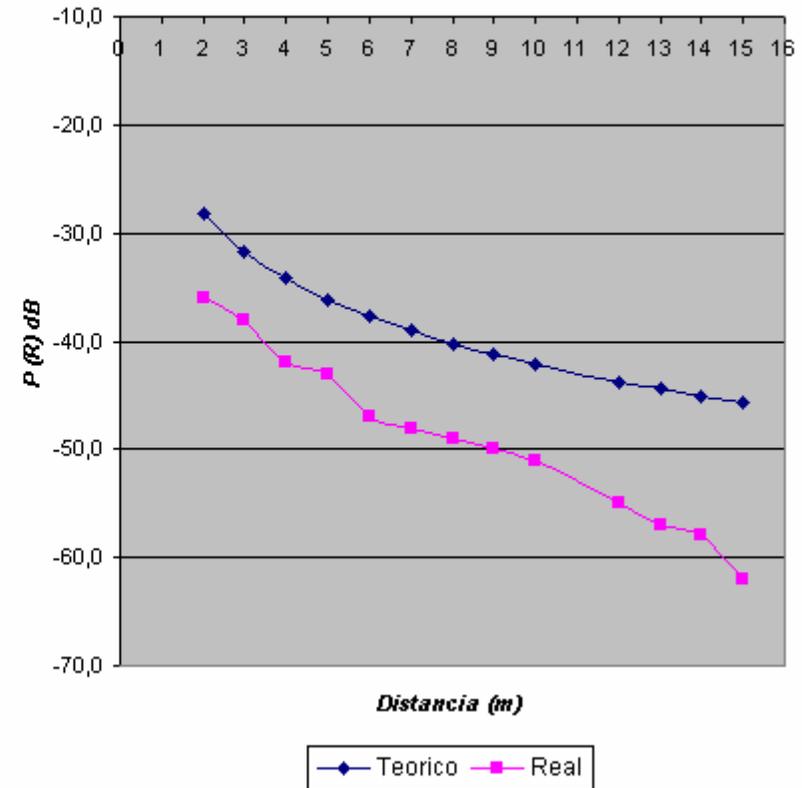
n MEDIO =	1,47703535	VARIANZA =	16,16853507
		DESVIACION =	4,02101170

$$\begin{aligned}
 \text{PTx (W)} &= 0,06200 \\
 \text{Gt} &= 1,00000 \\
 \text{Gr} &= 1,00000 \\
 \text{? (m)} &= 0,12438 \\
 \text{L} &= 1,00000
 \end{aligned}$$

Valores de n - Biblioteca



Valores de $P(R)$ - Biblioteca

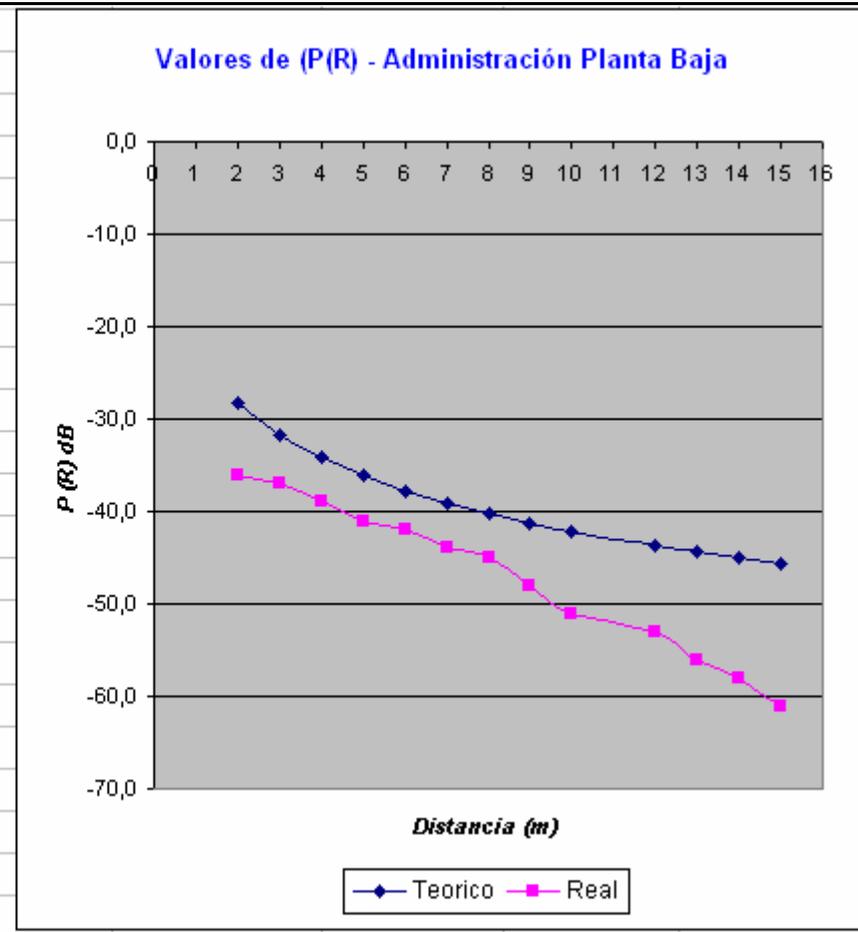
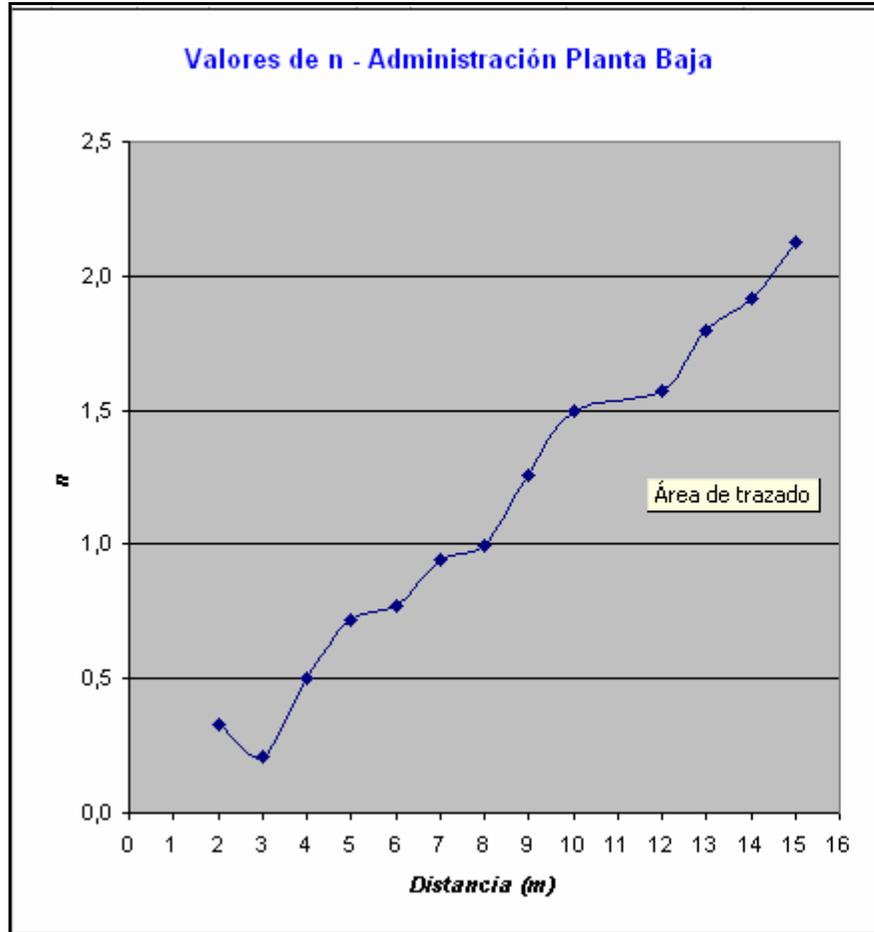


ADMINISTRACIÓN-PLANTA BAJA

d0	PL(do)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)
1	-35	-36	2	<i>n= 0,33219281</i>	2,39078068	55,39459551	46,10991817	46,63794351	0,0000015184	-28,18600127
1	-36	-37	3	<i>n= 0,20959033</i>	4,37426023	57,69772684	49,63174335	46,95759530	0,0000006749	-31,70782645
1	-36	-39	4	<i>n= 0,49828921</i>	3,78156137	59,31835309	52,13051808	47,17092041	0,0000003796	-34,20660119
1	-36	-41	5	<i>n= 0,71533828</i>	2,87314893	60,56848099	54,06871834	47,32946075	0,0000002430	-36,14480145
1	-36	-42	6	<i>n= 0,77105833</i>	2,76504092	61,58574678	55,65234326	47,45483455	0,0000001687	-37,72842637
1	-36	-44	7	<i>n= 0,94663573</i>	1,51912484	62,44308019	56,99127906	47,55808404	0,0000001240	-39,06736216
1	-36	-45	8	<i>n= 0,99657843</i>	1,17234205	63,18379405	58,15111800	47,64558069	0,0000000949	-40,22720110
1	-36	-48	9	<i>n= 1,25754196</i>	-1,25147953	63,83571341	59,17416844	47,72132164	0,0000000750	-41,25025155
1	-36	-51	10	<i>n= 1,50000000</i>	-3,73607038	64,41777369	60,08931826	47,78797277	0,0000000607	-42,16540136
1	-36	-53	12	<i>n= 1,57526829</i>	-4,84417840	65,42263965	61,67294318	47,90094674	0,0000000422	-43,74902628
1	-36	-56	13	<i>n= 1,79542344</i>	-7,45262048	65,86288190	62,36818530	47,94963108	0,0000000359	-44,44426841
1	-36	-58	14	<i>n= 1,91950631</i>	-9,09009447	66,27000114	63,01187897	47,99422430	0,0000000310	-45,08796207
1	-36	-61	15	<i>n= 2,12568538</i>	-11,75259083	66,64861250	63,61114344	48,03533202	0,0000000270	-45,68722654

n MEDIO =	<i>1,12639296</i>	VARIANZA =	<i>28,79257487</i>
		DESVIACION =	<i>5,36587131</i>

PTx (W) =	<i>0,06200000</i>
Gt =	<i>1,00000000</i>
Gr =	<i>1,00000000</i>
? (m) =	<i>0,12437811</i>
L =	<i>1,00000000</i>



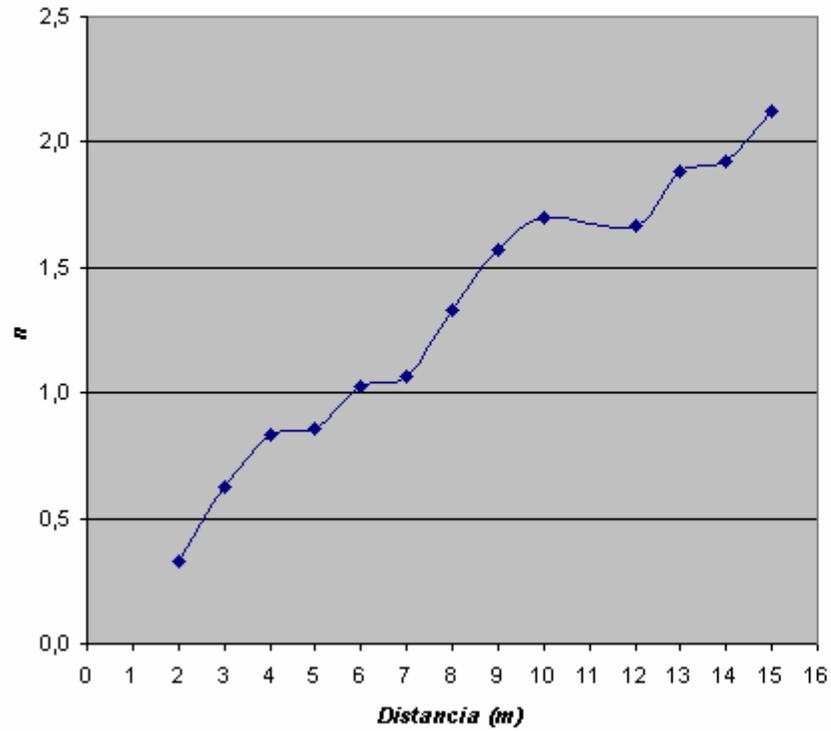
FILOSOFIA PLANTA BAJA

d0	PL(do)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)
1	-38	-39	2	n= 0,33219281	2,92309488	55,07622210	46,10991817	46,63794351	0,0000015184	-28,18600127
1	-38	-41	3	n= 0,62877098	3,21795828	57,69073728	49,63174335	46,95759530	0,0000006749	-31,70782645
1	-38	-43	4	n= 0,83048202	2,84618977	59,53229388	52,13051808	47,17092041	0,0000003796	-34,20660119
1	-38	-44	5	n= 0,85840593	3,10914423	60,95378868	54,06871834	47,32946075	0,0000002430	-36,14480145
1	-38	-46	6	n= 1,02807777	2,14105316	62,11107141	55,65234326	47,45483455	0,0000001687	-37,72842637
1	-38	-47	7	n= 1,06496520	2,01351973	63,08678747	56,99127906	47,55808404	0,0000001240	-39,06736216
1	-38	-50	8	n= 1,32877124	-0,23071535	63,93004904	58,15111800	47,64558069	0,0000000949	-40,22720110
1	-38	-53	9	n= 1,57192746	-2,56408345	64,67242189	59,17416844	47,72132164	0,0000000750	-41,25025155
1	-38	-55	10	n= 1,70000000	-3,96776089	65,33539558	60,08931826	47,78797277	0,0000000607	-42,16540136
1	-38	-56	12	n= 1,66793113	-3,93585196	66,48027849	61,67294318	47,90094674	0,0000000422	-43,74902628
1	-38	-59	13	n= 1,88519461	-6,48282388	66,98199090	62,36818530	47,94963108	0,0000000359	-44,44426841
1	-38	-60	14	n= 1,91950631	-7,06338539	67,44602261	63,01187897	47,99422430	0,0000000310	-45,08796207
1	-38	-63	15	n= 2,12568538	-9,67289749	67,87761823	63,61114344	48,03533202	0,0000000270	-45,68722654

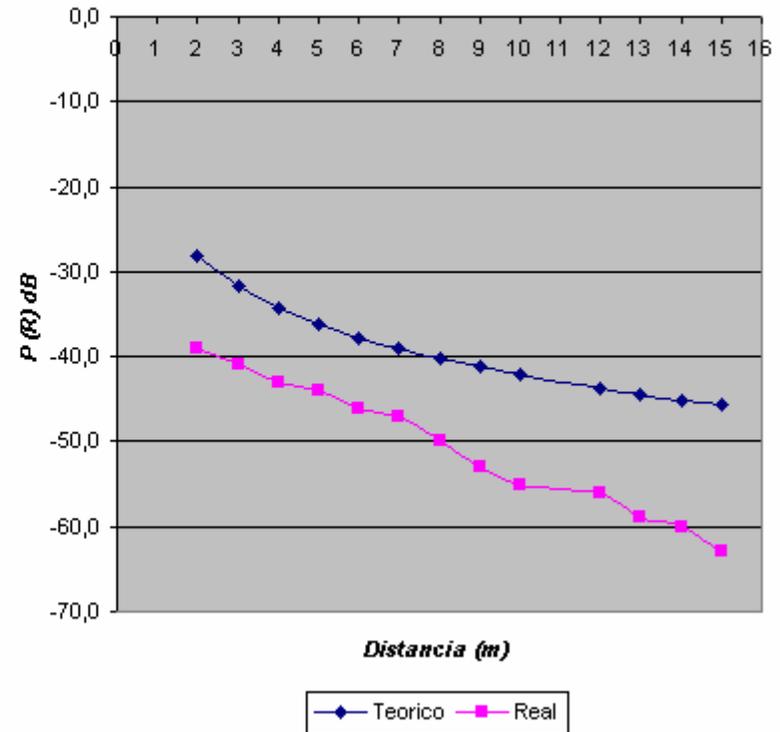
n MEDIO =	1,30322391	VARIANZA =	20,38688383
		DESVIACION =	4,51518370

PTx (W) =	0,06200000
Gt =	1,00000000
Gr =	1,00000000
? (m) =	0,12437811
L =	1,00000000

Valores de n - Filosofia Planta Baja



Valores de P(R) - Filosofia Planta Baja

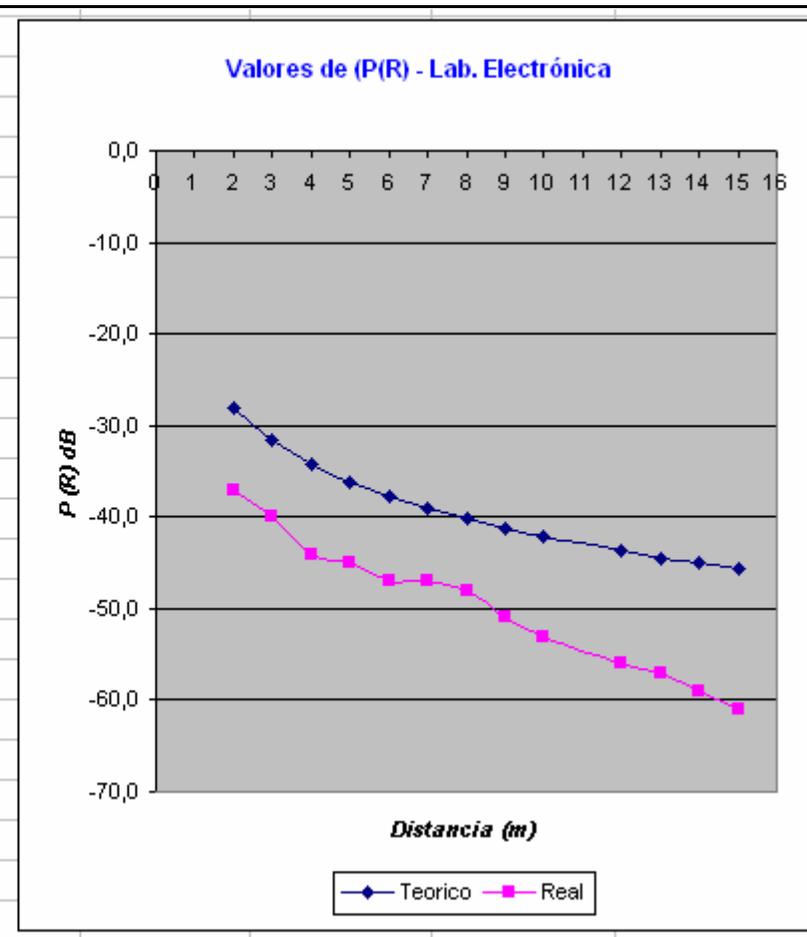
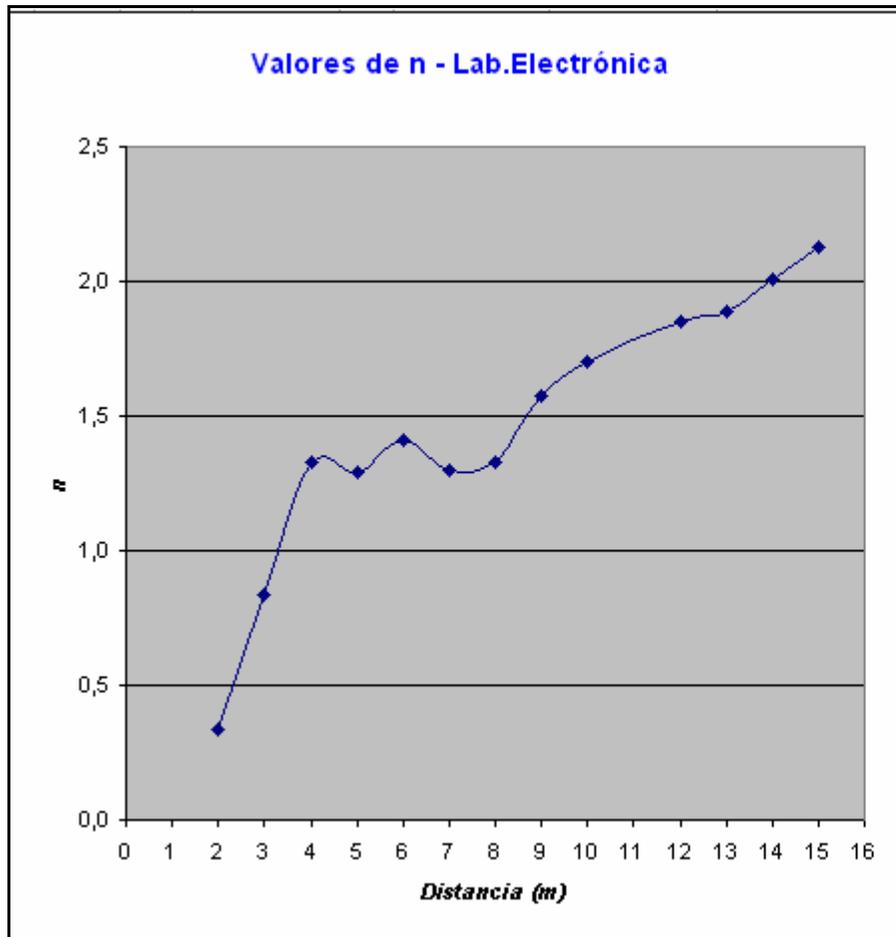


LABORATORIO DE ELECTRONICA

d0	PL(do)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)
1	-36	-37	2	n= 0,33219281	3,39359239	54,63384732	46,10991817	46,63794351	0,0000015184	-28,18600127
1	-36	-40	3	n= 0,83836131	2,96367919	57,52358590	49,63174335	46,95759530	0,0000006749	-31,70782645
1	-36	-44	4	n= 1,32877124	0,78718479	59,56041661	52,13051808	47,17092041	0,0000003796	-34,20660119
1	-36	-45	5	n= 1,28760890	1,20160562	61,13337778	54,06871834	47,32946075	0,0000002430	-36,14480145
1	-36	-47	6	n= 1,41360693	0,35727158	62,41441755	55,65234326	47,45483455	0,0000001687	-37,72842637
1	-36	-47	7	n= 1,30162413	1,33437324	63,49476868	56,99127906	47,55808404	0,0000001240	-39,06736216
1	-36	-48	8	n= 1,32877124	1,18077718	64,42866928	58,15111800	47,64558069	0,0000000949	-40,22720110
1	-36	-51	9	n= 1,57192746	-1,07264162	65,25099143	59,17416844	47,72132164	0,0000000750	-41,25025155
1	-36	-53	10	n= 1,70000000	-2,40480199	65,98548219	60,08931826	47,78797277	0,0000000607	-42,16540136
1	-36	-56	12	n= 1,85325682	-4,24913602	67,25412213	61,67294318	47,90094674	0,0000000422	-43,74902628
1	-36	-57	13	n= 1,88519461	-4,74177620	67,81016629	62,36818530	47,94963108	0,0000000359	-44,44426841
1	-36	-59	14	n= 2,00675660	-6,27203437	68,32450134	63,01187897	47,99422430	0,0000000310	-45,08796207
1	-36	-61	15	n= 2,12568538	-7,83471519	68,80292824	63,61114344	48,03533202	0,0000000270	-45,68722654

n MEDIO = 1,45951980	VARIANZA = 12,97664749
	DESVIACION = 3,60231141

PTx (W) = 0,06200000
Gt = 1,00000000
Gr = 1,00000000
? (m) = 0,12437811
L = 1,00000000



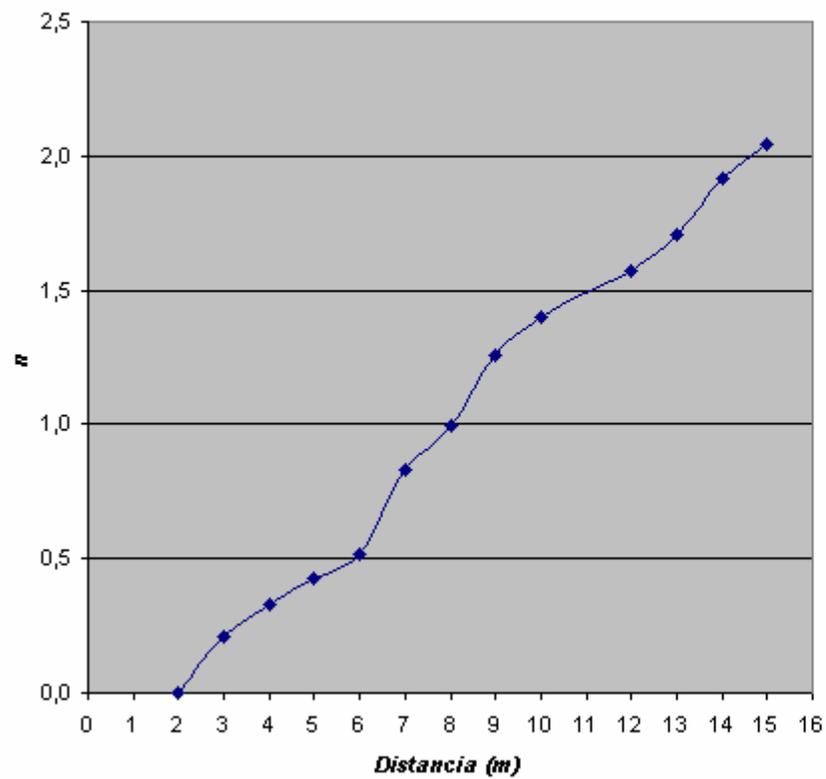
FACULTAD DE DISEÑO

d0	PL(do)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)
1	-36	-36	2	n= 0,00000000	3,05858898	55,52891348	46,10991817	46,63794351	0,0000015184	-28,18600127
1	-36	-37	3	n= 0,20959033	3,84774885	57,63772513	49,63174335	46,95759530	0,0000006749	-31,70782645
1	-36	-38	4	n= 0,33219281	4,11717797	59,12047936	52,13051808	47,17092041	0,0000003796	-34,20660119
1	-36	-39	5	n= 0,42920297	4,10182369	60,26366542	54,06871834	47,32946075	0,0000002430	-36,14480145
1	-36	-40	6	n= 0,51403888	3,90633783	61,19355336	55,65234326	47,45483455	0,0000001687	-37,72842637
1	-36	-43	7	n= 0,82830626	1,58654484	61,97700986	56,99127906	47,55808404	0,0000001240	-39,06736216
1	-36	-45	8	n= 0,99657843	0,17576695	62,65372862	58,15111800	47,64558069	0,0000000949	-40,22720110
1	-36	-48	9	n= 1,25754196	-2,30450231	63,24920031	59,17416844	47,72132164	0,0000000750	-41,25025155
1	-36	-50	10	n= 1,40000000	-3,83958732	63,78076643	60,08931826	47,78797277	0,0000000607	-42,16540136
1	-36	-53	12	n= 1,57526829	-6,03507318	64,69825454	61,67294318	47,90094674	0,0000000422	-43,74902628
1	-36	-55	13	n= 1,70565226	-7,68187584	65,10013622	62,36818530	47,94963108	0,0000000359	-44,44426841
1	-36	-58	14	n= 1,91950631	-10,35486617	65,47173911	63,01187897	47,99422430	0,0000000310	-45,08796207
1	-36	-60	15	n= 2,04065797	-12,05042746	65,81728554	63,61114344	48,03533202	0,0000000270	-45,68722654

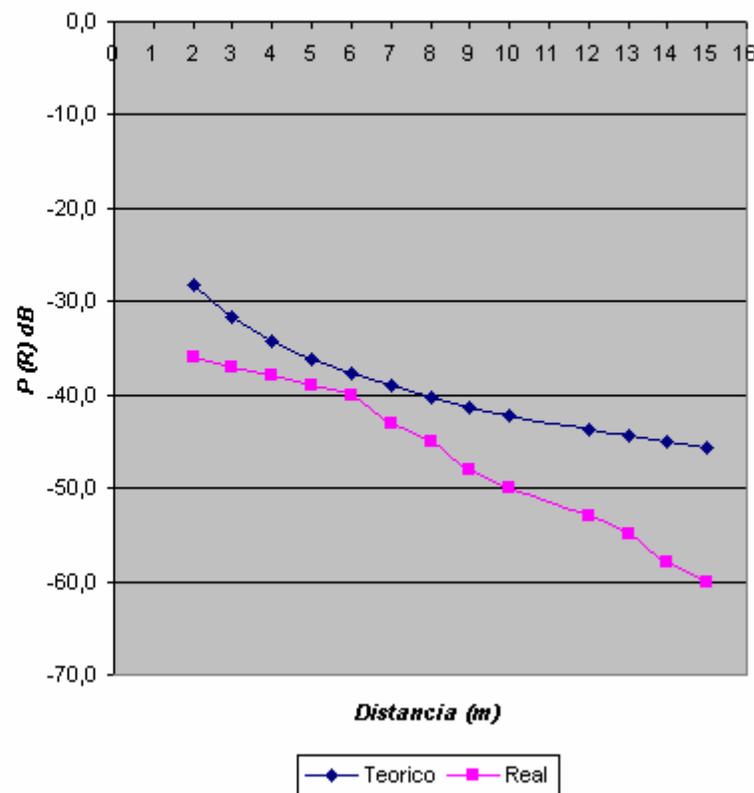
n MEDIO =	1,01604127	VARIANZA =	34,01666789
		DESVIACION =	5,83238098

PTx (W) =	0,06200000
Gt =	1,00000000
Gr =	1,00000000
? (m) =	0,12437811
L =	1,00000000

Valores de n - FACULTAD DE DISEÑO



Valores de $P(R)$ - FACULTAD DE DISEÑO



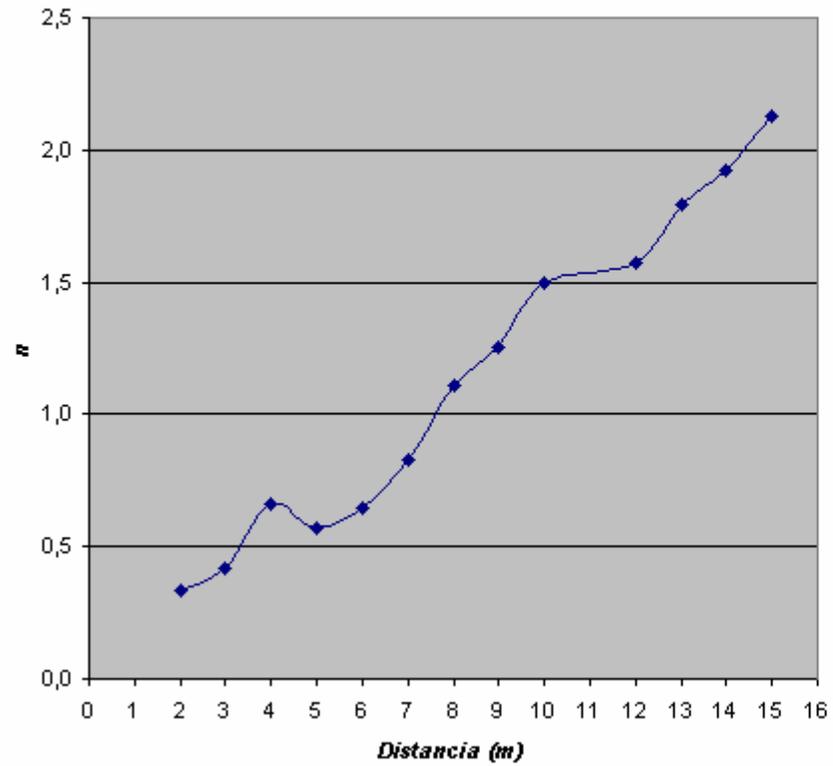
FACULTAD DE CIENCIAS Y TECNOLOGIA

d0	PL(d0)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)
1	-38	-39	2	n= 0,33219281	2,41312888	55,41328438	46,10991817	46,63794351	0,0000015184	-28,18600127
1	-38	-40	3	n= 0,41918065	3,40968128	57,72948857	49,63174335	46,95759530	0,0000006749	-31,70782645
1	-38	-42	4	n= 0,66438562	2,82625776	59,35939016	52,13051808	47,17092041	0,0000003796	-34,20660119
1	-38	-42	5	n= 0,57227062	3,92503984	60,61671257	54,06871834	47,32946075	0,0000002430	-36,14480145
1	-38	-43	6	n= 0,64254860	3,82281016	61,63985670	55,65234326	47,45483455	0,0000001687	-37,72842637
1	-38	-45	7	n= 0,82830626	2,58186416	62,50216018	56,99127906	47,55808404	0,0000001240	-39,06736216
1	-38	-48	8	n= 1,10730936	0,23938664	63,24717931	58,15111800	47,64558069	0,0000000949	-40,22720110
1	-38	-50	9	n= 1,25754196	-1,18063743	63,90289619	59,17416844	47,72132164	0,0000000750	-41,25025155
1	-38	-53	10	n= 1,50000000	-3,66183128	64,48835347	60,08931826	47,78797277	0,0000000607	-42,16540136
1	-38	-55	12	n= 1,57526829	-4,76406096	65,49909777	61,67294318	47,90094674	0,0000000422	-43,74902628
1	-38	-58	13	n= 1,79542344	-7,36992233	65,94192073	62,36818530	47,94963108	0,0000000359	-44,44426841
1	-38	-60	14	n= 1,91950631	-9,00500696	66,35142933	63,01187897	47,99422430	0,0000000310	-45,08796207
1	-38	-63	15	n= 2,12568538	-11,66527888	66,73226513	63,61114344	48,03533202	0,0000000270	-45,68722654

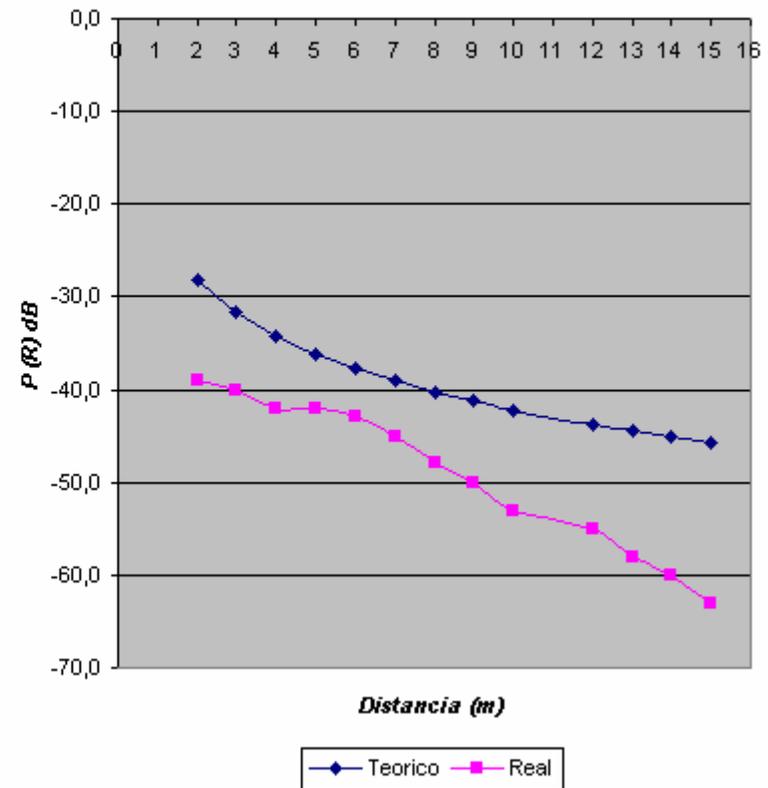
n MEDIO =	1,13381687	VARIANZA =	28,75331738
		DESVIACION =	5,36221199

PTx (W) =	0,06200000
Gt =	1,00000000
Gr =	1,00000000
? (m) =	0,12437811
L =	1,00000000

Valores de n - Ciencias y Tecnología



Valores de $P(R)$ - Ciencias y Tecnología



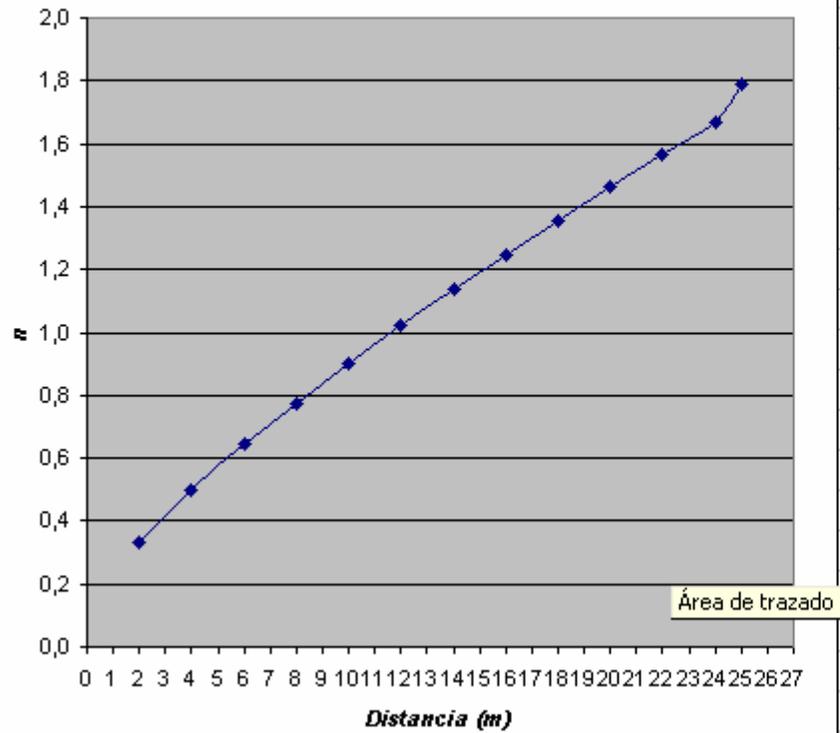
DECANATO DE INVESTIGACION Y SALA DE COMPUTO

d0	PL(do)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)
1	-35	-36	2	<i>n= 0,33219281</i>	<i>2,33012751</i>	<i>54,48284581</i>	<i>46,10991817</i>	<i>46,63794351</i>	<i>0,0000015184</i>	<i>-28,18600127</i>
1	-35	-38	4	<i>n= 0,49828921</i>	<i>3,66025503</i>	<i>58,34595022</i>	<i>52,13051808</i>	<i>47,17092041</i>	<i>0,0000003796</i>	<i>-34,20660119</i>
1	-35	-40	6	<i>n= 0,64254860</i>	<i>3,60825474</i>	<i>60,57786408</i>	<i>55,65234326</i>	<i>47,45483455</i>	<i>0,0000001687</i>	<i>-37,72842637</i>
1	-35	-42	8	<i>n= 0,77511656</i>	<i>2,99038254</i>	<i>62,15073801</i>	<i>58,15111800</i>	<i>47,64558069</i>	<i>0,0000000949</i>	<i>-40,22720110</i>
1	-35	-44	10	<i>n= 0,90000000</i>	<i>2,06244415</i>	<i>63,36519170</i>	<i>60,08931826</i>	<i>47,78797277</i>	<i>0,0000000607</i>	<i>-42,16540136</i>
1	-35	-46	12	<i>n= 1,01929125</i>	<i>0,93838226</i>	<i>64,35410379</i>	<i>61,67294318</i>	<i>47,90094674</i>	<i>0,0000000422</i>	<i>-43,74902628</i>
1	-35	-48	14	<i>n= 1,13425373</i>	<i>-0,32102262</i>	<i>65,18797646</i>	<i>63,01187897</i>	<i>47,99422430</i>	<i>0,0000000310</i>	<i>-45,08796207</i>
1	-35	-50	16	<i>n= 1,24572304</i>	<i>-1,67948995</i>	<i>65,90872149</i>	<i>64,17171791</i>	<i>48,07343666</i>	<i>0,0000000237</i>	<i>-46,24780101</i>
1	-35	-52	18	<i>n= 1,35428761</i>	<i>-3,11361803</i>	<i>66,54328423</i>	<i>65,19476836</i>	<i>48,14212747</i>	<i>0,0000000187</i>	<i>-47,27085146</i>
1	-35	-54	20	<i>n= 1,46038139</i>	<i>-4,60742834</i>	<i>67,11001264</i>	<i>66,10991817</i>	<i>48,20266620</i>	<i>0,0000000152</i>	<i>-48,18600127</i>
1	-35	-56	22	<i>n= 1,56433591</i>	<i>-6,14952407</i>	<i>67,62196323</i>	<i>66,93777187</i>	<i>48,25671252</i>	<i>0,0000000125</i>	<i>-49,01385498</i>
1	-35	-58	24	<i>n= 1,66641158</i>	<i>-7,73149023</i>	<i>68,08875701</i>	<i>67,69354309</i>	<i>48,30547246</i>	<i>0,0000000105</i>	<i>-49,76962619</i>
1	-35	-60	25	<i>n= 1,78834570</i>	<i>-9,53536674</i>	<i>68,30756926</i>	<i>68,04811843</i>	<i>48,32816121</i>	<i>0,0000000097</i>	<i>-50,12420153</i>

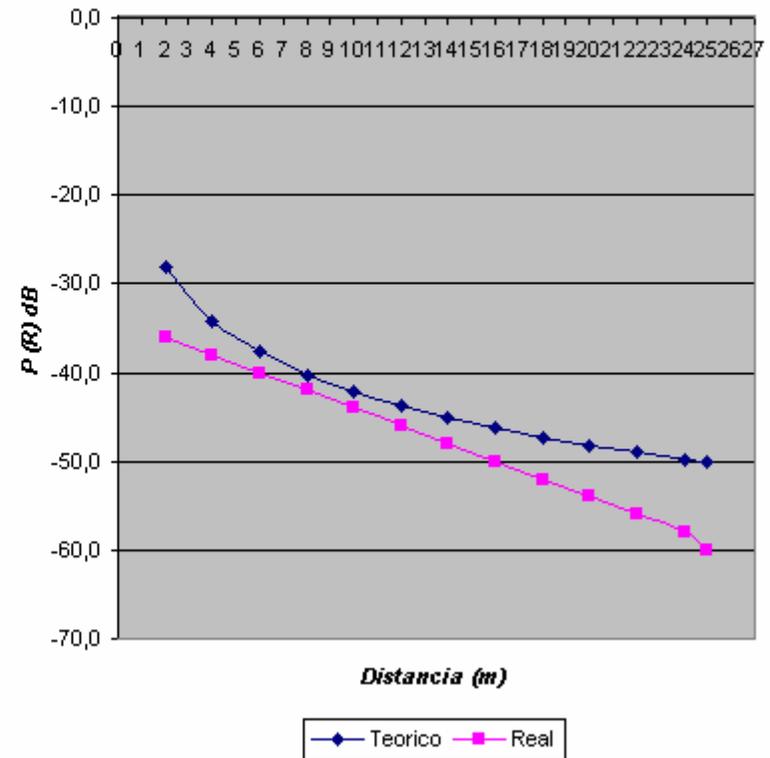
n MEDIO =	1,10624441	VARIANZA =	20,38319135
		DESVIACION =	4,51477478

PTx (W) =	0,06200000
Gt =	1,00000000
Gr =	1,00000000
? (m) =	0,12437811
L =	1,00000000

Valores de n - DECANATO DE INVESTIGACION Y SALA DE COMPUTO



Valores de $P(R)$ - DECANATO DE INVESTIGACION Y SALA DE COMPUTO



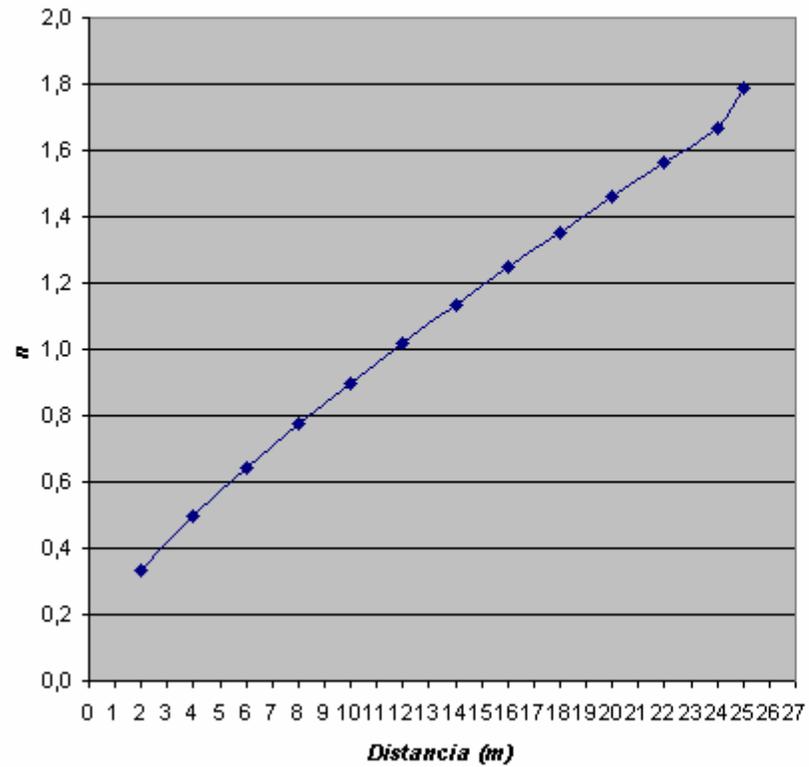
ADMINISTRACION CENTRAL

d0	PL(do)	PR(d)	Distancia (d)	n	Xs	P perdida de trayecto (R)	PL (w)	PL perdida (dB)	P (R) (W)	P recibida (R) (dB)
1	-35	-36	2	n= 0,33219281	2,33012751	54,48284581	46,10991817	46,63794351	0,0000015184	-28,18600127
1	-35	-38	4	n= 0,49828921	3,66025503	58,34595022	52,13051808	47,17092041	0,0000003796	-34,20660119
1	-35	-40	6	n= 0,64254860	3,60825474	60,57786408	55,65234326	47,45483455	0,0000001687	-37,72842637
1	-35	-42	8	n= 0,77511656	2,99038254	62,15073801	58,15111800	47,64558069	0,0000000949	-40,22720110
1	-35	-44	10	n= 0,90000000	2,06244415	63,36519170	60,08931826	47,78797277	0,0000000607	-42,16540136
1	-35	-46	12	n= 1,01929125	0,93838226	64,35410379	61,67294318	47,90094674	0,0000000422	-43,74902628
1	-35	-48	14	n= 1,13425373	-0,32102262	65,18797646	63,01187897	47,99422430	0,0000000310	-45,08796207
1	-35	-50	16	n= 1,24572304	-1,67948995	65,90872149	64,17171791	48,07343666	0,0000000237	-46,24780101
1	-35	-52	18	n= 1,35428761	-3,11361803	66,54328423	65,19476836	48,14212747	0,0000000187	-47,27085146
1	-35	-54	20	n= 1,46038139	-4,60742834	67,11001264	66,10991817	48,20266620	0,0000000152	-48,18600127
1	-35	-56	22	n= 1,56433591	-6,14952407	67,62196323	66,93777187	48,25671252	0,0000000125	-49,01385498
1	-35	-58	24	n= 1,66641158	-7,73149023	68,08875701	67,69354309	48,30547246	0,0000000105	-49,76962619
1	-35	-60	25	n= 1,78834570	-9,53536674	68,30756926	68,04811843	48,32816121	0,0000000097	-50,12420153

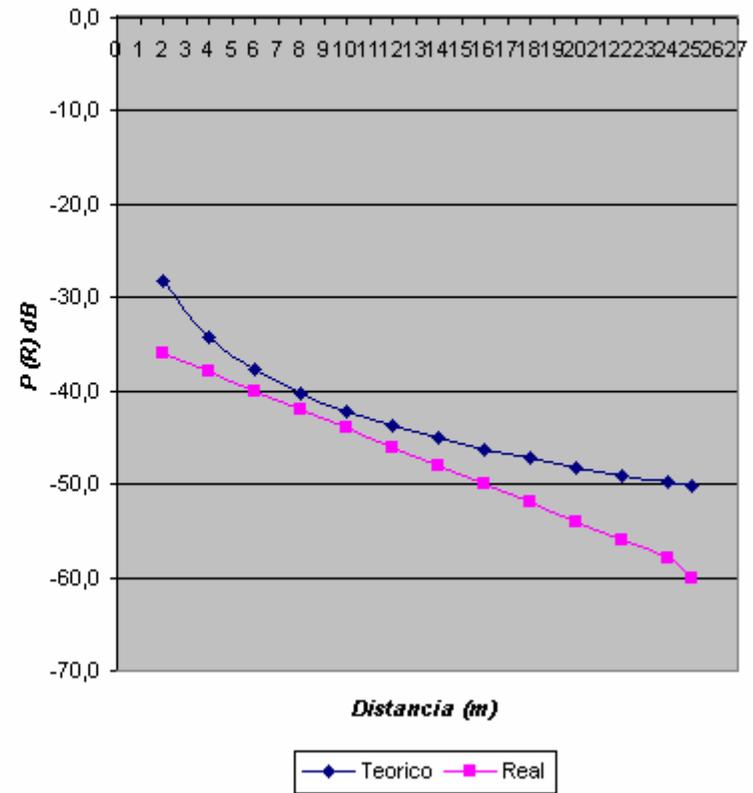
n MEDIO =	1,10624441	VARIANZA =	20,38319135
		DESVIACION =	4,51477478

PTx (W) =	0,06200000
Gt =	1,00000000
Gr =	1,00000000
? (m) =	0,12437811
L =	1,00000000

Valores de n - ADMINISTRACION CENTRAL



Valores de (P(R)) - ADMINISTRACION CENTRAL



RESUMEN DE CALCULOS

ENTORNO	n MEDIO	DESVIACION	VARIANZA
Biblioteca	1,47703535	4,02101170	16,16853507
Administración P.B.	1,12639296	5,36587131	28,79257487
Administración P1	1,31313623	3,78320642	14,31265078
Administración P2	1,08762859	6,17191058	38,09248021
Administración P3	1,18850047	4,53920925	20,60442060
Administración P4	1,28217694	4,07016493	16,56624254
Filosofía PB	1,30322391	4,51518370	20,38688383
Filosofía P1	1,41879866	3,14987461	9,92171007
Filosofía P2	1,29291479	4,85969592	23,61664444
Filosofía P3	1,54932581	4,06336224	16,51091271
Filosofía P4	1,29641201	5,53038580	30,58516706
Decanato de Investigaciones y Centro de Computo	1,10624441	4,51477478	20,38319135
Edificio de Administración Central	1,10624441	4,51477478	20,38319135
Facultad de Ciencias y Tecnología.	1,13381687	5,36221199	28,75331738
Facultad de Diseño	1,01604127	5,83238098	34,01666789
Laboratorio de Electronica	1,45951980	3,60231141	12,97664749

n promedio	1,25983828	
	Desviación Promedio	4,61852065