



**DISEÑO DE UNA WLAN PARA LA FUNDACIÓN
UNIVERSITARIA AGRARIA DE COLOMBIA
UNIAGRARIA**

**PRÁCTICA EMPRESARIAL
EN PRESING LTDA.**



GIOVANNY ARMANDO SERRANO CUADROS

**UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE
TELECOMUNICACIONES
BUCARAMANGA**

2006



***DISEÑO DE UNA WLAN PARA LA FUNDACIÓN
UNIVERSITARIA AGRARIA DE COLOMBIA
UNIAGRARIA***

GIOVANNY ARMANDO SERRANO CUADROS

Código: 1952670

Trabajo de Grado

Modalidad: Práctica Empresarial

Presentado como

requisito para optar al título de

Ingeniero Electrónico

Director

OSCAR MAURICIO REYES TORRES

UIS

Tutor

Ing. RICARDO MESA BARBOSA

PRESING LTDA

**UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE
TELECOMUNICACIONES
BUCARAMANGA**

2006

RESUMEN

TÍTULO: DISEÑO WLAN PARA LA FUNDACIÓN UNIVERSITARIA AGRARIA DE COLOMBIA UNIAGRARIA*

AUTOR: GIOVANNY ARMANDO SERRANO CUADROS **

Palabras clave: *Estudio del sitio, inalámbrico, cobertura, planeación, punto de acceso.*

Este trabajo presenta el diseño de una red de área local inalámbrica WLAN (Wireless Local Area Network) para la Fundación Universitaria Agraria de Colombia UNIAGRARIA, que aumentará la cobertura de la actual red cableada de datos y brindará mayor acceso a bases de datos, intranet e Internet. Se presenta un resumen de las tecnologías inalámbricas más relevantes y pertinentes para una implementación WLAN, como Bluetooth, WAP, WLAN 802.11x, y sus estándares, específicamente el 802.11g. Mediante la determinación de la topología y el estudio de la red de datos existente en cuanto a ubicación y clase de equipos, y un Estudio del Sitio (Site Survey) se determina la ubicación preliminar y el modo de trabajo de los diferentes puntos de acceso.

La Fundación Universitaria Agraria de Colombia UNIAGRARIA adelanta la ampliación y adecuación de su planta física como parte de las actividades en relación a la conmemoración de sus 20 años de fundada; con la construcción de cuatro nuevos edificios y la remodelación de la sede alterna ubicada en Tenjo. Es una necesidad para UNIAGRARIA tener disponibilidad, cobertura y acceso a Internet en la mayoría de su campus.

De manera que el presente trabajo demuestra que mediante una metodología de planeación responsable y rigurosa se logra un sistema óptimo en desempeño y cobertura. Además brinda una guía para el desarrollo e implementación de su red inalámbrica, ofreciendo flexibilidad y escalabilidad.

* Trabajo de Grado

** Facultad de Ingenierías Físico mecánicas, Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Oscar Mauricio Reyes Torres. Tutor: Ricardo Mesa Barbosa.

ABSTRACT

TITLE: WLAN DESIGN FUNDACION UNIVERSITARIA AGRARIA DE COLOMBIA UNIAGRARIA *

AUTHOR: GIOVANNY ARMANDO SERRANO CUADROS **

Key words: *Site Survey, Coverage, Planning, Access Point.*

This work presents Wireless LAN Network design for Fundación Universitaria Agraria de Colombia UNIAGRARIA, which will increase coverage of current wired data network and will offer mayor access to data base, intranet and Internet. It presents a resume of most important wireless technologies for a WLAN implementation, like Bluetooth, WAP, WLAN 802.11x, and your standards, specifically 802.11g. Trough topology determining and existing data network study about location and kinds of devices, and Site Survey Study it determines the previous location and work mode of different access points.

The Fundación Universitaria Agraria de Colombia UNIAGRARIA advances execution enlargement labor of your facilities as part of related activities to celebration your 20th anniversary; with the construction of four new buildings and remodelation of alternative branch of Tenjo. It is a needing for UNIAGRARIA gets availability, coverage and access to Internet in the most of installations.

By mean present work, it demonstrates that trough methodology of responsible and rigorous planning; it obtains an optimal system about performance and coverage. Besides it gives a guide to development and implementation of your wireless network, offering flexibility and scalability.

* Project of Grade

** Physic-Mechanic Engineers Faculty. Electrical, Electronic and Telecommunication's School
Director: Oscar Mauricio Reyes Torres. Tutor: Ricardo Mesa Barbosa.

AGRADECIMIENTOS

El autor expresa agradecimientos a:

A Presing Ltda.

A mis padres y familia.

A DIOS PADRE por sus innumerables oportunidades.

TABLA DE CONTENIDO

	Pág.
RESUMEN	IV
AGRADECIMIENTOS	VI
LISTA DE TABLAS	VIII
LISTA DE FIGURAS	IX
GLOSARIO	X
INTRODUCCION	1
1. ESTUDIO DE LAS TECNOLOGIAS INALÁMBRICAS PARA REDES DE ÁREA LOCAL	3
2. ESTUDIO DE LA TOPOLOGÍA Y EQUIPOS DE RED EXISTENTES EN UNIAGRARIA	4
3. ESTUDIO DE LA UBICACIÓN GEOGRÁFICA DE LAS INSTALACIONES	8
3.1. REQUERIMIENTOS Y PARÁMETROS DE DISEÑO	9
3.2. MÉTODO ESTUDIO DE SITIO (SITE SURVEY)	15
4. CONCLUSIONES Y RECOMENDACIONES	41
REFERENCIAS BIBLIOGRÁFICAS	43
ANEXOS	45
ANEXO A. TECNOLOGÍA BLUETOOTH	45
A.1. Usos y aplicaciones Bluetooth	46
A.2. Estándares y Protocolos	48
A.3. Seguridad	51
ANEXO B. TECNOLOGÍA WAP	54
B.1. Usos y aplicaciones WAP	54
B.2. Estándares y Protocolos	56
B.3. Seguridad	61
ANEXO C. TECNOLOGÍA WLAN	63
C.1. Usos y Aplicaciones WLAN	65
C.2. Estándares y Protocolos	67
Estándar 802.11	67
Estándar 802.11a	70
Estándar 802.11b	71
Estándar 802.11g	72
C.3. Seguridad	73
ANEXO D. OTRAS TECNOLOGIAS INALÁMBRICAS	78
D.1. Tecnología HomeRF 2.0	78
D.2. Tecnología HiperLAN2	78
D.3. Tecnología Wi-Max	79
ANEXO E. REQUERIMIENTOS DE DISEÑO DE UNA WLAN Y MÉTODO SITE SURVEY	81
ANEXO F. PLANO ESQUEMÁTICO RED LÓGICA UNIAGRARIA	86
ANEXO G. ALGUNAS HERRAMIENTAS SOFTWARE MONITOR WLANs	87
ANEXO H. ESPECIFICACIONES DISPOSITIVOS INALÁMBRICOS	88
ANEXO I. PRESING LTDA	94

LISTA DE TABLAS

	Pág.
Tabla 2.1. Equipos red de datos UNIAGRARIA	5
Tabla 3.1. Cronograma actividades	14
Tabla 3.2. Cobertura <i>Outdoor</i> AP Linksys WRT54G	18
Tabla 3.3. Cobertura <i>Indoor</i> AP Linksys WRT54G	18
Tabla 3.4. Cobertura <i>Outdoor</i> TrendNet TEW 430 APB	19
Tabla 3.5. Cobertura <i>Indoor</i> TrendNet TEW 430 APB	19
Tabla 3.6. Disponibilidad y desvanecimiento del enlace	21
Tabla 3.7. Atenuación de potencia por material de construcción	22
Tabla 3.8. Distancias óptimas de STA al AP Linksys	24
Tabla 3.9. Distancias óptimas de STA al AP TrendNet	25
Tabla 3.10. Máximos teóricos throughput	33
Tabla 3.11. Prueba1 AP Linksys sistemas/sala Internet	34
Tabla 3.12. Prueba2 AP Linksys Biblioteca	35
Tabla 3.13. Prueba3 AP Deportes modo WDS	37
Tabla 3.14. Equipos a utilizar	39
Tabla 3.15. Costos estimados	40
Tabla A.1. Parámetros de Radio y Banda Base Bluetooth	49
Tabla C.1. Comparación de Tecnologías Inalámbricas según categorías	64
Tabla C.2. Variantes de 802.11	73
Tabla D.1. Comparación 802.11b con otras tecnologías	80
Tabla E.1 Interferencia de las ondas RF	84

LISTA DE FIGURAS

	Pág.
Figura 2.1. Esquema red de datos UNIAGRARIA	6
Figura 3.1. Vista superior UNIAGRARIA	8
Figura 3.2. Ubicación Física equipos de red UNIAGRARIA	9
Figura 3.3. Posibles ubicaciones para los APs	10
Figura 3.4. Fotografía entrada cafetería	10
Figura 3.5. Fotografía corredor principal	11
Figura 3.6. Fotografía entrada Oficina Profesores y Auditorio	11
Figura 3.7. Dibujo entrada Oficina Profesores y Auditorio	11
Figura 3.8. Fotografía construcción edificio de cuatro pisos	12
Figura 3.9. Dibujo fachada sur y occidental edificio cuatro pisos	12
Figura 3.10. Áreas de cobertura LAN y WLAN	13
Figura 3.11. Fotografía fachada norte Biblioteca	15
Figura 3.12. Fotografía cancha de fútbol	16
Figura 3.13. Fotografía Edificio Postgrados	16
Figura 3.14. Fotografía cancha múltiple	17
Figura 3.15. Cobertura inalámbrica deseada	17
Figura 3.16. Comparación alcances Indoor v/s. Outdoor AP Linksys	19
Figura 3.17. Comparación alcances Indoor v/s. Outdoor AP TrendNet	19
Figura 3.18. Enlace AP Linksys – STA	20
Figura 3.19. Enlace AP TrendNet – STA	24
Figura 3.20. División espacial UNIAGRARIA	26
Figura 3.21. Cobertura Factor Z	27
Figura 3.22. Ubicación APs según Factor Z	27
Figura 3.23. Zona de Fresnell para WDS	28
Figura 3.24. Ubicación APs	31
Figura 3.25 (a). Consola Check	32
Figura 3.25 (b). Consola NetStumbler	32
Figura 3.25 (c). Consola NetStumbler	33
Figura 3.26. Verificación AP Linksys sistemas/sala Internet	34
Figura 3.27. Throughput vs. Fuerza de la señal prueba1	35
Figura 3.28. Verificación AP Linksys Biblioteca	35
Figura 3.29. Throughput vs. Fuerza de la señal prueba2	36
Figura 3.30. Verificación AP Linksys Deportes modo WDS	37
Figura 3.31. Throughput vs. Fuerza de la señal prueba3	38
Figura 3.32. Esquema red inalámbrica UNIAGRARIA	39
Figura A.1. Esquema general <i>piconet</i> Bluetooth	46
Figura A.2. Pila de Protocolos Bluetooth	51
Figura A.3 (a) Proceso Autenticación Bluetooth. Inicio de diálogo	52
Figura A.3. (b) Proceso Autenticación Bluetooth. Respuesta y comparación	52
Figura B.1. Infraestructura WAP	57
Figura B.2. Ejemplo de una red WAP	58
Figura B.3. Pila de Protocolos WAP	61
Figura C.1. Etiqueta Wi-Fi	68
Figura C.2. Modelo red Ad Hoc	69
Figura C.3. Modelo red Infraestructura	70
Figura C.4. Distribución de canales en la banda 2.4 GHz	72
Figura C.5. Panel de Configuración de Seguridad Firewall en un APR Linksys	75
Figura C.6. Autenticación 802.1x y servidor RADIUS	77

GLOSARIO

Access Point (AP): Es un componente de una red WLAN que realiza básicamente repetición de la señal. Es un punto de acceso de la red, que puede funcionar en una red Ethernet como hub, como switch, router, bridge u otros modos de trabajo dependiendo el modelo.

Ad-Hoc: Es uno de los modos de trabajo de un red WLAN donde no existen dispositivos intermedios administradores de la comunicación. Se conoce también como red Per-to-Per.

Antena: Parte de un sistema transmisor o receptor que está diseñada para radiar o recibir ondas electromagnéticas.

Atenuación: Reducción de la fuerza de una señal como una función de la distancia viajada.

Ancho de banda: capacidad de transmisión de un canal. Indica la cantidad de datos por unidad de tiempo que puede enviarse a través de una línea de transmisión, medida frecuentemente en bits por segundos (bps). También se refiere a la banda comprendida por la diferencia entre la frecuencia inferior y la superior de un canal de comunicaciones, medido en Hertz (Hz).

Backbone: Mecanismo de conectividad primario en un sistema distribuido. Todos los sistemas que tengan conexión al backbone (columna vertebral) pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas.

Bridge: Dispositivos que tienen usos definidos como interconectar segmentos de red a través de medios físicos diferentes (es usual ver puentes entre un cable coaxial y otro de fibra óptica). Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y capa física del modelo OSI).

Broadcast: Es una técnica utilizada para enviar paquetes de datos de manera simultánea a todos los dispositivos de un segmento de red.

Canal: Es un simple camino de transmisión de señales eléctricas. La palabra camino es para ser interpretada en un sentido extenso para incluir separación por división de frecuencia o división de tiempo. El término canal puede significar también un camino de una vía o de doble vía.

DHCP (Dynamic Host Configuration Protocol): servidor que se encarga de asignar los parámetros que requiere un PC para tener acceso a una red, entre ellos la dirección IP, la puerta de enlace dinámicamente.

Espectro ensanchado: Es una técnica en la cual la información en una señal es repartida o esparcida sobre un ancho de banda más grande del ancho de banda de la información empleando un código independiente al de los datos llamado código de esparcimiento, que es una secuencia de datos usada para esparcir el ancho de banda en un sistema de espectro esparcido.

Ethernet: Norma o estándar (IEEE 802.3) que determina la forma en que los adaptadores de red envían y reciben datos sobre un medio físico compartido que se comporta como un

bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps.

Fast Ethernet: Ethernet de alta velocidad (100 Mbps, para diferenciar de la Ethernet regular de 10 Mbps).

Firewall: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o mas partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.

Gigabit ethernet: también conocida como GigE, es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo que en la práctica se convierten en unos 100 megabytes útiles (Fast Ethernet tiene alrededor de 10).

Hub: Es un punto de conexión para diversos componentes de una red (pueden ser equipos, print servers, etc.). El Hub tiene muchos puertos, cuando recibe un paquete por uno lo envía a todos los otros, de forma de ser recibido por las demás terminales. Los hay inteligentes (se puede monitorizar el tráfico de cada puerto, configurarlo, etc.), y los pasivos que solamente conectan.

Infraestructura: Otro modo de operación o estructura de redes WLAN. Un dispositivo central administra las comunicaciones. Por lo general este dispositivo es un Access Point (AP).

ISM: (Industrial, Scientific and Medical). Banda de frecuencias de uso libre, asignada por estados unidos para aplicaciones de tipo industrial, medico y científico. Abarca las frecuencias de 900 MHz, 2.4 GHz, 5 GHz, donde se desarrollan los sistemas de espectro ensanchado como WLAN y Bluetooth.

MAC (Medium Access Control): Sistema de control de acceso al medio para dispositivos hardware en sistemas inalámbricos, basados en una dirección física de 48 bits.

OSI: Modelo de referencia de siete capas o niveles definido por la ISO, donde los tres niveles inferiores representan comunicaciones locales y las cuatro superiores comunicaciones extremas a extremo.

Piconet: Es un red Bluetooth formada por dos o más dispositivos equipados con un chip Bluetooth. Se requiere que un dispositivo maestro, y uno o más esclavos establezcan una conversación.

Radius: esquema de seguridad adicional de las redes WLAN que hace uso de un servidor equipado con una base de datos para autenticación de los usuarios móviles.

Roaming: es un concepto utilizado en comunicaciones wireless que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra sin la interrupción del servicio ni pérdidas de conectividad. Es una palabra de procedencia inglesa que significa vagar o vagabundear.

En telefonía celular es un sistema mediante el cual el teléfono se va conectando de manera automática a las células que le permitan una mejor comunicación. Existe un sistema de 'roaming' internacional mediante el cual se pueden realizar llamadas y recibirlas con el mismo número de teléfono de manera igual a la de la red original.

Router: Dispositivo usado para enlazar una o mas redes. El router hace uso de un protocolo Internet, el cual es un protocolo sin conexión operando en la capa 3 del modelo OSI.

RJ45: interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho 'pines' o conexiones eléctricas.

Servidor: Tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al equipo físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Sniffer: programa que monitorea y analiza el tráfico de una red para detectar problemas o cuellos de botella. Su objetivo es mantener la eficiencia del tráfico de datos. Pero también puede ser usado ilegítimamente para capturar datos en una red.

STP: Shielded Twisted Pair. Cable par trenzado apantallado.

Switch: dispositivo de interconexión de redes de equipos que opera en la capa 2(nivel de enlace de datos) del modelo OSI (Open Systems Interconnection). Este interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.

UTP: Unshielded Twisted Pair. Cable par trenzado sin apantallar. Tiene en sus principales ventajas: movilidad, facilidad de crecimiento y expansión, integración a altas velocidades de transmisión de datos compatibles con todas las LAN que soporten velocidades superiores a 100 Mbps.

VLAN: acrónimo de Virtual Local Area Network o Virtual LAN. Este concepto, consiste en cada una de las redes de área local creadas en los conmutadores, de forma que el tráfico de las distintas redes dentro del mismo switch no se mezcla entre ellas gracias a los mecanismos de enrutado.

VPN: (Virtual Private Network) Red privada virtual. Red de comunicaciones de área ancha provista por una portadora común que suministra aquello que asemeja líneas dedicadas cuando se utilizan, pero las troncales de base se comparten entre todos los clientes como en una red pública. Permite configurar una red privada dentro de una red pública.

Wireless. Se refiere a la transmisión a través del aire, del vacío o agua, por el medio o por una antena.

INTRODUCCIÓN

Hace mucho tiempo las comunicaciones inalámbricas dejaron de ser ajenas en el entorno nacional. Conocerlas es imperativo para cualquier institución o entidad educativa, más aún utilizarlas, es una posibilidad abierta y una premisa inaplazable, ya que permanecer aislado de aplicaciones de este tipo es limitar los medios disponibles para el desempeño productivo o académico según sea el caso.

Actualmente UNIAGRARIA adelanta un proyecto de ampliación de sus locaciones que implícitamente incluye la ampliación de personal docente y personal administrativo y se hace necesario la expansión de su red de datos. Por esto frente a la necesidad de extensión y cubrimiento, se requiere una solución a corto plazo viable que aproveche los actuales recursos de red y alternativa a una solución cableada, la cual aumentaría los costos en obras civiles en espacios como parqueaderos y zonas deportivas.

De manera que esta alternativa es una red de datos inalámbrica que descongestione y agilice el acceso a bases de datos, especialmente Internet e intranet, ofreciendo movilidad, procesamiento y generación de cualquier tipo de información. También es necesario dimensionarla debido a las numerosas peticiones de acceso inalámbrico a Internet por parte del estudiantado y al creciente número de dispositivos electrónicos vistos con acceso wireless, por parte de estudiantes y profesorado como laptops*, PDAs¹ y equipos celulares.

UNIAGRARIA y PRESING Ltda. han mantenido un vínculo comercial como cliente y proveedor de tecnología respectivamente donde este estudio de diseño hace parte de un valor agregado en una licitación para adquisición de equipos de red, equipos inalámbricos, de seguridad, adecuaciones y mobiliario. PRESING Ltda en su proceso de actualización en tecnologías inalámbricas demanda ingenieros electrónicos, para el estudio, diseño, implementación y puesta en marcha de proyectos de esta índole.

En el contenido de este libro se encuentra un estudio de tecnologías inalámbricas, referencia de los equipos a utilizar, recomendaciones y sugerencias de seguridad, esquema gráfico del diseño, planteamiento del diseño realizado y esta organizado en cuatro capítulos. En el Capítulo 1 se hace una breve mención de las diferentes tecnologías inalámbricas predominantes y se hace la remisión a los ANEXOS A, B y C para conocerlas en detalle. En el Capítulo 2 se presenta la recopilación de las topologías física, lógica y equipos de red de datos en las instalaciones de UNIAGRARIA, para tener una concepción previa del comportamiento de la red sin hacer análisis de tráfico. El Capítulo 3 trata la metodología y pasos del diseño, teoría que se puede estudiar en el ANEXO E. Aquí se consignaron los datos de las diferentes mediciones y verificaciones hechas así como el esquema y planteamiento final de diseño, logrado mediante una planeación responsable y argumentada.

El resultado final es este documento que contiene el diseño de una red de área local inalámbrica WLAN para la Fundación Universitaria Agraria de Colombia

* Computador Portátil.

¹ Personal Digital Assistant.

UNIAGRARIA, que sirve como referencia y soporte para UNIAGRARIA y para PRESING LTDA en futuros diseños, implementaciones y trabajos de este tipo.

1. ESTUDIO DE LAS TECNOLOGIAS INALÁMBRICAS PARA REDES DE ÁREA LOCAL

Las tecnologías inalámbricas han entrado en gran auge en los últimos años brindando a los usuarios comodidad y libertad aunque aun están distantes de reemplazar las redes cableadas. Factores como la falta de confianza a implantar tecnologías nuevas, la ausencia de normas, han contribuido a que los sistemas inalámbricos no obedezcan a las expectativas de crecimiento esperado. Sin embargo, su importancia e interés aumenta día a día siendo una de las más prometedoras tecnologías, importancia que se ha visto reflejada con la aparición de dispositivos electrónicos tanto para oficina como para el hogar tales como computadoras digitales, celulares, PDAs, cámaras wireless, adaptadores inalámbricos para video juegos como Play Station, XBox, estereos o equipos de sonido, audífonos wireless, así como la necesidad y requerimiento de aplicaciones inalámbricas en la industria y el comercio. También se ha visto reflejada en su implementación en las grandes capitales del mundo donde los gobiernos locales y estatales han brindado cobertura inalámbrica a la totalidad o a la mayoría del área de estas. Bucaramanga es la única ciudad de Colombia que posee este servicio, gracias a un programa llamado Bucaramanga inalámbrica se brinda actualmente cobertura a la ciudad y área metropolitana excepto Piedecuesta.

Las tecnologías del tipo inalámbrico destacan dos segmentos importantes:

- Telefonía móvil o celular.
- Redes de área local inalámbricas, WLAN (Wireless Local Area Network).

La telefonía móvil o celular se ha posicionado en el mercado de las telecomunicaciones y han experimentado un crecimiento exponencial, tanto en la calidad del servicio, como en el número de usuarios. En nuestro país existen tres empresas operadoras de telefonía celular y se espera que el Ministerio de Comunicaciones abra una nueva licitación para un cuarto operador. Por el contrario, las WLAN se encuentran en un periodo de inserción y desarrollo. Si bien en EE.UU. Europa y Japón este tipo de tecnología ya está implementada, se espera que pronto tenga una mayor penetración en los ámbitos laborales tanto industriales como comerciales.

Actualmente existen tres tecnologías inalámbricas con gran aceptación en el mercado, ofreciendo todas acceso inalámbrico pero desarrollándose en campos de acción determinados. Estas tecnologías son: BLUETOOTH, WAP (Wireless Application Protocol) y WLAN (Wireless Local Area Network).

Información detallada en cuanto a estándares, protocolos, usos, aplicaciones, seguridad, en los anexos A, B y C respectivamente. En el Anexo D se mencionan otras tecnologías y alternativas existentes.

2. ESTUDIO DE LA TOPOLOGÍA Y EQUIPOS DE RED EXISTENTES EN UNIAGRARIA

La red de datos de la Fundación Agraria de Colombia UNIAGRARIA, esta basada en la tecnología Fast Ethernet 100 Mbps y tiene una topología de estrella extendida.

El centro de la estrella se encuentra en el Centro de Sistemas en la sala de Sistemas 3. Cuenta con tres Switches Core marca 3Com de 24 puertos, con funcionalidades de capa 2 y capa 3 conectados a 1000BaseSX; fibra óptica multimodo de 62.5 micrómetros a 1 Gbps. Estos Switches Core están ubicados en Sistemas 3, en Biblioteca y en Consejo Superior ubicado en la parte de Administración. Estos Switches Core se comunican con los diferentes Switches Edge² o Switches de Borde ubicados en las diferentes dependencias mediante cableado UTP CAT 5E. La conexión a los usuarios finales es también mediante par trenzado UTP CAT 5E. El enlace WAN es un enlace E1, que conecta al ISP, ETB.³ Tiene tres equipos servidores marca Hewllet Packard y un equipo firewall marca 3Com, router marca Cisco y tiene 175 usuarios en su red con equipos en su mayoría marca Dell.

El sistema operativo utilizado para la administración de la red es Windows Server 2003 y en los usuarios finales es Windows XP. Esta red de datos no tiene una plataforma tecnológica definida, pues a pesar de tener mayoría de equipos marca 3Com, tiene equipos de otras marcas como Cisco, TrendNet, LG, lo que le da un carácter de red híbrida en cuanto a soporte tecnológico.

La red presenta una topología plana y direccionamiento IP clase C, 192.168.1.0 con máscara de red 255.255.255.0.

Es importante mencionar como equipos que dan soporte a la red de datos los equipos de regulación y administración de potencia como equipos de regulación de voltaje y equipos como Unidades Ininterrumpidas de Potencia UPSs.

La distribución de los equipos de red es como sigue y se muestra en la **Tabla 2.1**.

Un esquema de la red de datos se muestra en la **Figura 2.1**.

ROUTER / UBICACIÓN	CANTIDAD	MARCA Y REFERENCIA
Dirección Sistemas	1	Cisco Series 1700
SWITCHES CORE / UBICACIÓN	CANTIDAD	MARCA Y REFERENCIA
Sala Sistemas 3	1	3Com Super Stack 3 Sw 4228G x24
Biblioteca	1	3Com Super Stack 3 Sw 4228G x24
Consejo Superior	1	3Com Super Stack 3 Sw 4228G x24

² Significa límite. En el contexto de redes de datos se refiere a switches de borde o de frontera.

³ Empresa de Telecomunicaciones de Bogotá.

SWITCHES EDGE / UBICACIÓN	CANTIDAD	MARCA Y REFERENCIA
Sala Internet	1	LG LGLS3116A Switch x16
Oficinas Profesores	1	TrendNet Switch TE100-S32+ x32
Ingenierías	1	TrendNet TE100 S88E Mini Sw N-Way x8
Laboratorios	2	TrendNet TE100-S16 Switch 10/100 x 16
Secretaría Postgrados	1	3Com SuperStack 3 Sw 3300 x24
Derecho	1	TrendNet TE100 S88E Mini Sw N-Way x8
Bienestar Universitario	1	3Com Office Connect Dual Speed Switch 16 Plus
Registro y Control	1	TrendNet TE100 S88E Mini Sw N-Way x8
Tesorería	1	TrendNet TE100 S88E Mini Sw N-Way x8
Contabilidad	1	TrendNet TE100 S88E Mini Sw N-Way x8
HUBS / UBICACIÓN	CANTIDAD	MARCA Y REFERENCIA
Sala Sistemas 1	2	3Com Office Connect Hub 16
Sala Sistemas 2	1	3Com Office Connect Hub 16
Sala Sistemas 3	1	3Com Super Stack II Hub x24
Deportes	1	3Com Office Connect Hub 16
FIREWALL / UBICACIÓN	CANTIDAD	MARCA Y REFERENCIA
Dirección Sistemas	1	3Com SuperStack 3 Port LAN/DMZ/WAN
SERVIDORES / UBICACIÓN	CANTIDAD	MARCA Y REFERENCIA
Dirección sistemas	3	HP Net Server LC2000

Tabla 2.1. Equipos red de datos UNIAGRARIA

Fuente: Autor

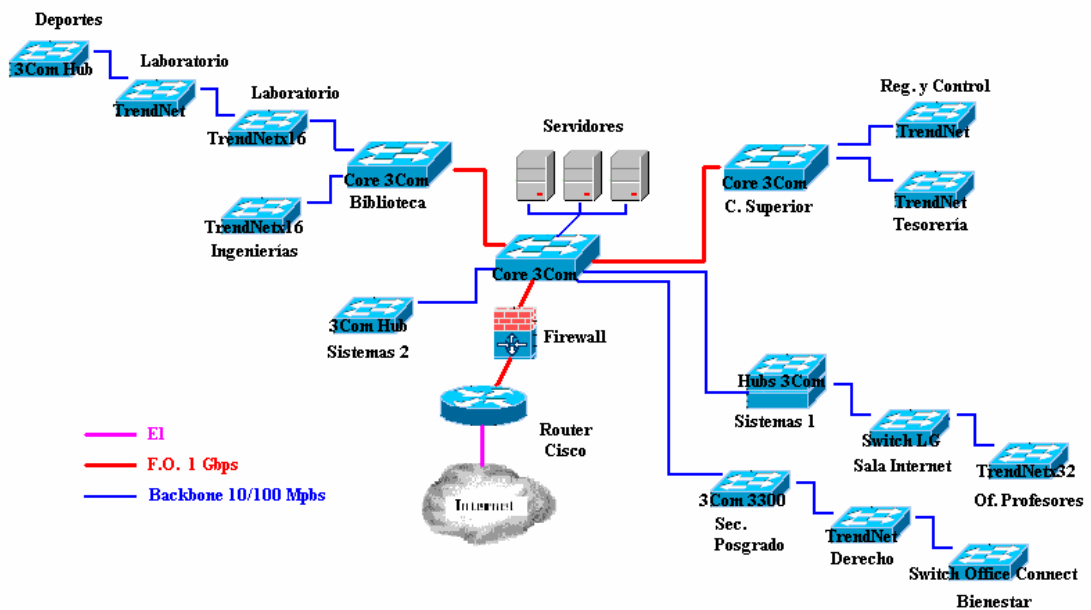


Figura 2.1. Esquema red de datos UNIAGRARIA
Fuente: Autor

Como observación y valoración preliminar los Switches Core 3Com 4228G no están configurados adecuadamente pues funcionan con su característica plug-and-play y se valen de su autosensing para distribuir la velocidad y ancho de banda a los dispositivos, la red no tiene por ejemplo definidos grupos de trabajo, para dependencias administrativas importantes como tesorería o contabilidad. Aunque su desempeño no es malo, no es el óptimo para las prestaciones que brinda esta familia de switches.

Otra observación esta en la ubicación de hubs en puntas iniciales de la estrella, seguidos luego por switches, esto disminuye el desempeño de la red de manera considerable. Estas inconsistencias tanto en implementación como en variedad de marcas comerciales en la red de datos se deben al crecimiento continuo de la planta física y a una inadecuada planeación en la escalabilidad debida a diferentes administraciones. Sin embargo, esto no es impedimento para diseñar sobre esta red una implementación inalámbrica traducida en más segmentaciones de red y en instalación de dispositivos inalámbricos, sin riesgo de inundar la red. La topología de estrella extendida y forma de operación brinda aún flexibilidad y escalabilidad. No existirá problema de compatibilidad entre los dispositivos inalámbricos y los dispositivos e infraestructura de la red cableada.

Como presenta una topología de estrella extendida, y la tendencia de esta estrella es extenderse aún más con las nuevas adecuaciones y construcciones de planta física, con seguridad se adquirirán más switches de borde. Los dispositivos inalámbricos o puntos de acceso APs a implementar se ubicarán en los switches de borde para asegurar la calidad del enlace inalámbrico y asegurar que el ancho de banda para cada AP sea dedicado. De todo esto se concluye que el modo de trabajo a elegir para la implementación de la WLAN será en *modo infraestructura*, además porque se quiere mayor cobertura y conectividad permanente.

Se puede aprovechar los switches de borde ubicados más a los extremos de la estrella extendida, para dar cobertura a las últimas áreas de la universidad donde no existe parte cableada ni conectividad alguna.

En el ANEXO H se muestra el plano esquemático de la red lógica UNIAGRARIA.

3. ESTUDIO DE LA UBICACIÓN GEOGRÁFICA DE LAS INSTALACIONES

Como paso primero y fundamental se consiguió la maqueta de la Universidad a escala 1:200.

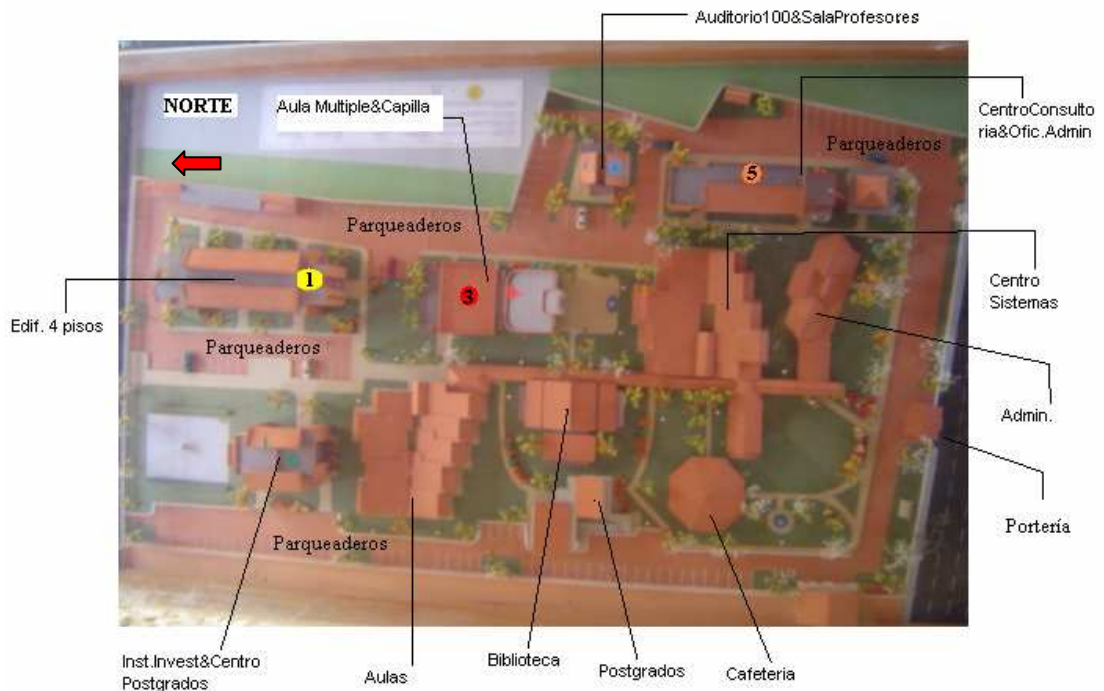


Figura 3.1. Vista superior UNIAGRARIA (Maqueta)

Fuente: UNIAGRARIA

Las instalaciones de la Fundación Universitaria Agraria de Colombia tienen un área aproximada de $(200\text{ m} * 300\text{ m}) = 60.000\text{ m}^2$, equivalente a 6 Hectáreas.

En esta fase del diseño se aplica el método Estudio de Sitio (*site survey*), pero primero se deben definir los requerimientos y parámetros de diseño.

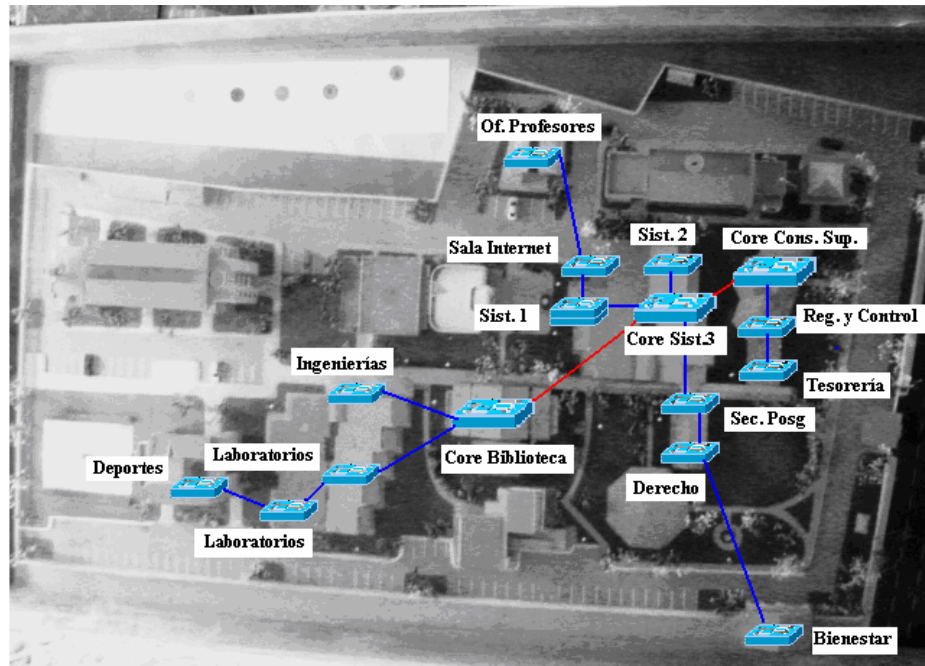


Figura 3.2. Ubicación Física equipos de red UNIAGRARIA

3.1. REQUERIMIENTOS Y PARÁMETROS DE DISEÑO.

Arquitectura. La planta física tiene casi todas las edificaciones de una planta, excepto el Edificio de Postgrados y las edificaciones que se están construyendo, que serán de cuatro plantas. La mayoría de los techos como el de Biblioteca y Administración son en madera y cubiertos en el exterior con teja de arcilla, pese a ser las tejas elementos que producen una atenuación media, en estos edificios se puede esperar una interferencia o atenuación baja de las ondas RF.

Las posibles ubicaciones para los APs de acuerdo a esta inspección de la arquitectura y planta física podrían ser:

1. Oficinas de Profesores
2. Asistencia de sistemas / Sala Internet
3. Consejo Superior
4. Derecho
5. Bienestar
6. Biblioteca
7. Ingenierías
8. Laboratorios de química aplicada
9. Deportes

En la **Figura 3.3.** se relacionan estas posibles ubicaciones.

Uno de los parámetros de diseño es brindar cobertura inalámbrica para acceso a Internet teniendo en cuenta los proyectos de ampliación de planta física adelantados.



Figura 3.3. Posibles ubicaciones para los APs

Actualmente esta proyectado y se adelanta lo siguiente:

- Auditorio para 100 personas dotado de nuevas tecnologías audiovisuales.
- Construcción de salas para 30 nuevos profesores de tiempo completo. Estos dos ítems anteriores están etiquetados en la maqueta con el número 2 en azul.
- Construcción y reubicación en la sede alterna de Tenjo del Laboratorio de morfología.
- Terminación y acabados de la planta piloto de alimentos y de los laboratorios de química básica y química aplicada.
- Construcción de un edificio de cuatro pisos con aulas y oficinas de postgrados. (Inicia en Diciembre de 2005 y se entrega a la comunidad académica en Julio de 2006). Número 1 en la maqueta **Figura 3.1.** en color amarillo.



Figura 3.4. Fotografía entrada cafetería
Fuente: Autor

El auditorio para 100 personas, las salas de profesores y los acabados en los laboratorios y planta piloto han sido finalizados. En el diseño no se tendrá en cuenta la sede alterna de Tenjo. La construcción del edificio de cuatro pisos aún esta en ejecución y se entregará hasta finales de este año.



Figura 3.5. Fotografía corredor principal
Fuente: Autor



Figura 3.6. Fotografía entrada Oficina Profesores y Auditorio
Fuente: Autor



Figura 3.7. Dibujo entrada Oficina Profesores y Auditorio
Fuente: Presing Ltda.



Figura 3.8. Fotografía construcción edificio de cuatro pisos
Fuente: Autor



Figura 3.9. Dibujo fachada sur y occidental edificio cuatro pisos
Fuente: Presing Ltda.

- **Aplicaciones.** Como uno de los objetivos es brindar acceso a Internet a la comunidad universitaria, especialmente a los estudiantes, las aplicaciones más usadas serían navegación Web y correos electrónicos. También consulta de libros en biblioteca. A nivel administrativo se piensan a futuro aplicaciones de vigilancia a través de cámaras IP y aplicaciones de transferencia de archivos. Se requiere entonces una buena velocidad de transmisión de datos.
- **Usuarios.** La UNIAGRARIA cuenta con una población universitaria de 1.500 aproximadamente, incluyendo personal administrativo, docente y de postgrados. La WLAN está pensada para dar servicio a usuarios móviles, aunque en la Oficina de Profesores todos los equipos de escritorio tienen tarjetas NIC inalámbricas. La cantidad de usuarios móviles en áreas de descanso y reunión como cafetería, canchas y zonas verdes se estima sea entre 15 y 30 usuarios simultáneamente para una sola celda. Se hace necesario establecer un direccionamiento IP dinámico DHCP.

- **Áreas de Cobertura.** En la **Figura 3.10.** se señalan en color morado las áreas donde llega la red cableada y en amarillo las áreas donde no existe conectividad alguna y donde se quiere cubrir con la WLAN. También se quiere tener y brindar cobertura adicional e inalámbrica en las áreas moradas para así en un 90 % del campus cualquier usuario móvil pueda acceder a Internet, esto como parámetro de diseño. Para nuestra región, la región de las Américas se usa la banda ISM de 2.4 GHz sin licencia y la banda de 5 GHz.

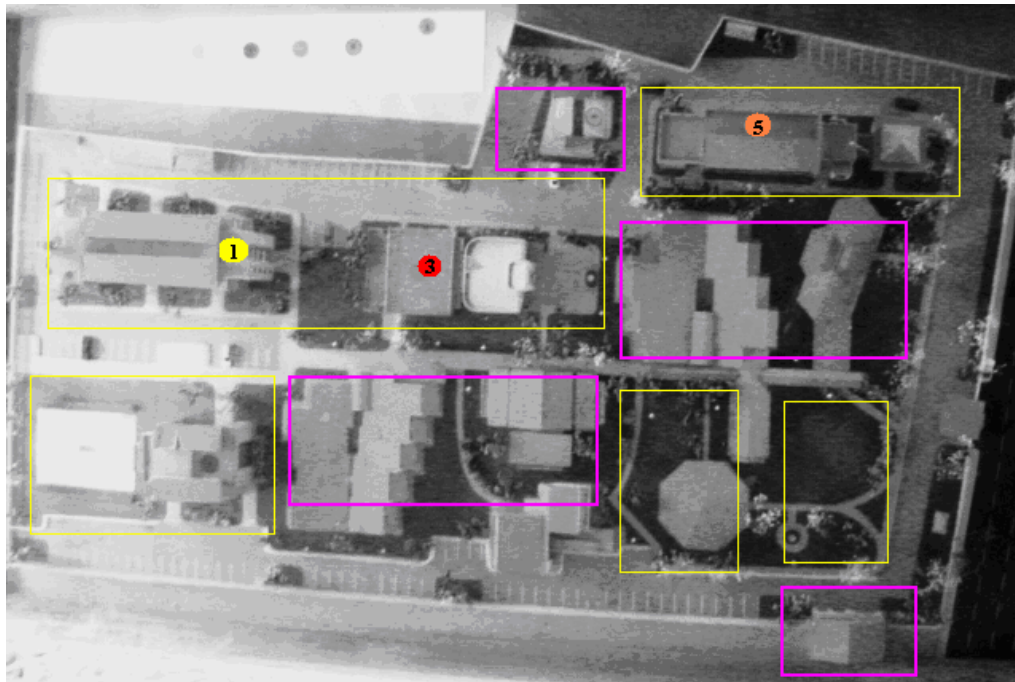


Figura 3.10. Áreas de cobertura LAN y WLAN

- **Seguridad.** Se desea evitar que algún usuario móvil invada en las aplicaciones administrativas como Registro y Control o Contabilidad, restringir el acceso a contenidos Web no académicos, e interceptación de información transmitida entre docentes. Para esto se aplicará cifrado WEP a 64 o 128 bits, dependiendo de los dispositivos a usar, también filtrado de direcciones MAC y la implementación de un software como el WebSense que restringe acceso a contenidos.
- **Dispositivos finales de usuario.** Las estaciones fijas o usuarios estacionarios, en su mayoría usan computadores marca Dell con procesadores Pentium III y Pentium IV bajo WindowsXP. Las estaciones de trabajo en Oficina de Profesores tienen tarjetas PCI TEW 403-PI 802.11g marca TredNet. Mediante un sondeo se encontró que los dispositivos inalámbricos como Palms y PDAs más usados por la comunidad universitaria son la T5 de Tungsten y la Palm Z22 con adaptadores Wi-Fi, procesadores de 200 MHz, memorias de 32 MB, sistemas operativos Palm OS 5.4, y computadores portátiles en su mayoría con tecnología Centrino. Además gran cantidad de teléfonos celulares con características Bluetooth y WAP.

- **Vida y duración de las baterías.** La administración de las baterías es inherente a cada usuario, tanto las baterías de sus portátiles, celulares y agendas digitales. Sin embargo algunos dispositivos AP poseen características de ahorro de energía *save energy* mientras se encuentran en inactividad.
- **Financiación.** La financiación para este proyecto no esta contemplada pues no se hará la implementación y el montaje de manera inmediata. El proyecto consta del diseño y dimensionamiento de la WLAN. Obviamente el estudio que se lleva a cabo como todo diseño, busca la mejor alternativa en economía.
- **Cronograma.** La entrega del documento final con el diseño de la WLAN y la duración están planificadas como sigue:

FASE / ACTIVIDAD	FECHAS	TIEMPO ESTIMADO
Fase1. Inducción y capacitación	Jueves 01 Diciembre de 2005 a Viernes 06 Enero de 2006.	27 días hábiles. Aprox. 5 semanas
Fase2 Estudio de las actuales tecnologías inalámbricas y productos existentes en el mercado	Lunes Enero 09 a Viernes 03 Febrero de 2006	20 días hábiles. 4 semanas
Fase 3. Estudio de la topología y equipos de red existentes en UNIAGRARIA.	Lunes 06 Febrero a Viernes 03 Marzo de 2006	20 días hábiles. 4 Semanas.
Fase 4. Estudio Ubicación geográfica de las instalaciones.	Lunes 06 Marzo a Viernes 28 Abril de 2006.	38 días hábiles. 8 Semanas
Fase 5. Diseño WLAN UNIAGRARIA	Lunes 01 Mayo a Viernes 02 Junio de 2006.	25 días hábiles. 5 Semanas

Tabla 3.1. Cronograma actividades

Teniendo claros los requerimientos y establecidos los parámetros de diseño, se aplica el método *site survey*, el cual nos dará la estimación del número y ubicación de puntos de acceso a utilizar. Se resumen entonces los lineamientos del diseño así:

- Cobertura del 90% del campus universitario. Aproximadamente 6 hectáreas.
- Roaming.
- Modo de operación infraestructura.
- Banda de frecuencias a usar: Banda ISM de 2.4 GHz.
- Velocidad de transmisión de datos 54 Mbps.
- Tecnología: WLAN 802.11g.
- Cantidad de usuarios por celda, aproximadamente 30.
- Nivel de seguridad 3, Seguridad mejorada, clave dinámica, autenticación 802.1x, EAP, WEP a 128 bits.
- Direccionamiento IP DHCP.

3.2. MÉTODO ESTUDIO DE SITIO (SITE SURVEY.)

- **Adquirir un plano o maqueta del lugar**

Se obtuvo una maqueta a escala 1:200. Se puede ver en la **Figura 3.1**.

- **Inspección visual**

Mediante una inspección visual se determinaron posibles fuentes de interferencia como unos árboles presentes en algunos espacios abiertos del campus, y entre algunos edificios, no existen hornos microondas, dispositivos bluetooth, teléfonos inalámbricos o motores; también se estimó posibles ubicaciones para los dispositivos inalámbricos teniendo en cuenta facilidades de red eléctrica y de red de datos. La altura promedio de las dependencias administrativas, sistemas, decanaturas e ingenierías, aulas y laboratorios es de 5 metros, 2.5 metros los pasillos y de 6 metros la biblioteca. Como su arquitectura es homogénea, las paredes y muros son alrededor de 10 y 15 centímetros respectivamente. Como se mencionó antes se espera bajas atenuaciones por la clase de materiales. En esta inspección se detectó la posible necesidad de realizar una implementación en modo *bridge* o modo WDS entre Biblioteca, Sistemas 3, Ingenierías o Deportes y el edificio de cuatro pisos, número 1 en amarillo en la maqueta.

Algunas fotos de las instalaciones en las siguientes Figuras:



Figura 3.11. Fotografía fachada norte Biblioteca
Fuente: Autor



Figura 3.12. Fotografía cancha de fútbol
Fuente: Autor



Figura 3.13. Fotografía Edificio Postgrados
Fuente: Autor



Figura 3.14. Fotografía cancha múltiple
Fuente: Autor

- **Identificación del área de cobertura**

En la maqueta, **Figura 3.1.** aparecen edificios como los enumerados con los números 1 en amarillo (edificio de cuatro pisos), número 3 en rojo (aula múltiple y capilla) y 5 en naranja (edificio centro de consultoría y administrativo), los cuales esta proyectada su construcción a partir del año 2007, excepto el número 5 que está en ejecución. En estos espacios existe un área abierta sin edificaciones, en el área del edificio número 3 que es el área encerrada en el recuadro verde de la **Figura. 3.15.** actualmente existe una cancha de fútbol y algunos árboles. La otra zona es el área encerrada por la elipse naranja.

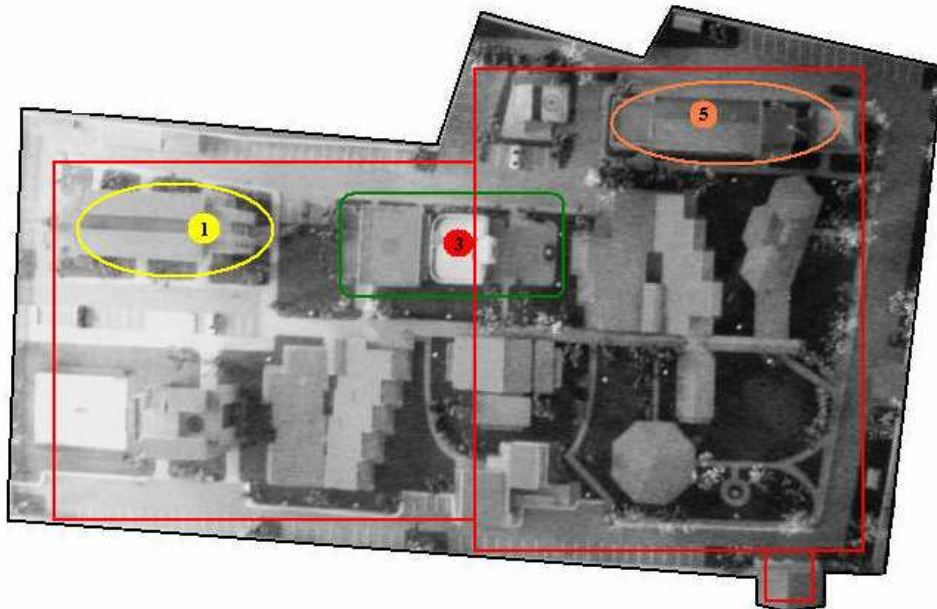


Figura 3.15. Cobertura inalámbrica deseada

Los recuadros rojos encierran el área de cobertura inalámbrica deseada estimada en una 90 %, dejando el 10 % restante en las zonas de perimetrales de parqueaderos y límites del campus.

- **Ubicación preliminar de los AP**

Primero una verificación de manera empírica de la real cobertura y alcance de los APs. Para la prueba se utilizó un AP de Linksys WRT54G y un AP de TrendNet TEW 430 APB y una tarjeta adaptador PCMCIA TEW 401 PC de TrendNet, suministrados por la Universidad, equipos que había adquirido antes y no estaban en uso, y un computador portátil.

Nominalmente tienen cobertura de 100 m y 400 m *indoor* y *outdoor* respectivamente según el estándar 802.11 El TEW 430 APB en sus especificaciones dice que alcanza distancias entre 50 m y 100 m *indoor* y de 100 m a 300 m *outdoor*.

Las especificaciones del WRT54G dicen que hasta 150 m *indoor* y 350m *outdoor*.

Las dimensiones del campus son aproximadamente de 200 x 300 m, lo que podría indicar que con uno o dos puntos de acceso ubicados en la mitad se obtendría un cubrimiento mínimo del 80 %. Las mediciones para cada AP en ambiente *indoor* y *outdoor* se muestran en las siguientes tablas:

Distancia (m)	Velocidad de transmisión (Mbps)
1	54
5	54
15	54
37	54
47	48
59	36
68	24
85	18
110	12
130	9
162	6
175	6

Tabla 3.2. Cobertura *Outdoor* AP Linksys WRT54G

Distancia (m)	Velocidad de transmisión (Mbps)
1	54
4	54
11	48
19	36
24	24
27	18
33	12
40	9
45	6
53	6
57	0

Tabla 3.3. Cobertura *Indoor* AP Linksys WRT54G

Distancia (m)	Velocidad de transmisión (Mbps)
1	54
5	54
14	48
37	36
47	24
61	18
68	12
90	9
120	6
127	0

Tabla 3.4. Cobertura *Outdoor* AP TrendNet TEW 430 APB

Distancia (m)	Velocidad de transmisión (Mbps)
1	54
4	54
7	48
11	36
15	24
19	18
24	12
27	9
31	6
36	0

Tabla 3.5. Cobertura *Indoor* AP TrendNet TEW 430 APB

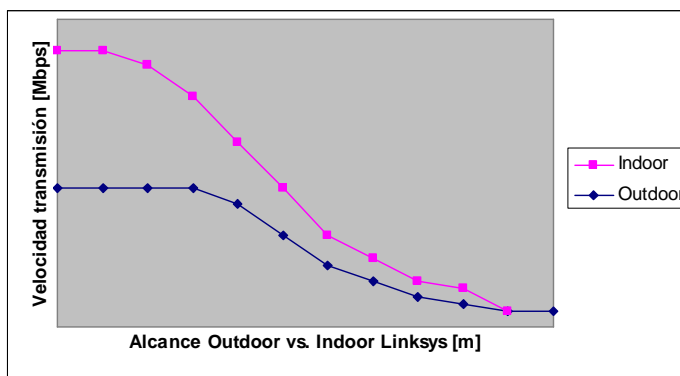


Figura 3.16. Comparación alcances Indoor v/s. Outdoor AP Linksys

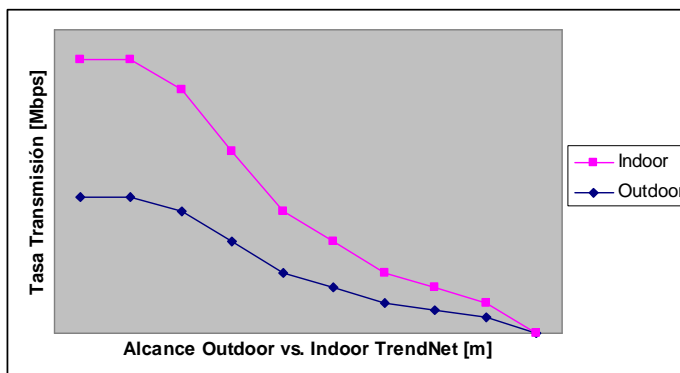


Figura 3.17. Comparación alcances Indoor v/s. Outdoor AP TrendNet

En la dos últimas Figuras se aprecia el obvio y mejor comportamiento en condiciones Outdoor para ambos APs. En ambientes Indoor decae más rápido su rango de cobertura, mientras que en ambientes outdoor se tienen mejores distancias a mejores y constantes velocidades de transmisión. El AP Linksys presenta un mejor desempeño en cuanto a cobertura que el AP TrendNet. Se juzga que la cobertura real no alcanzará la cobertura dada por las especificaciones técnicas de cada producto.

Las mediciones outdoor se realizaron colocando los APs en la esquina norte de la sala de Internet y alejándose en línea recta hasta el fondo del campus, a través de la cancha de fútbol hasta llegar a la cancha múltiple. Esta primera prueba se hizo con el comando 'ping' de DOS que es el comando 'echo' entre estaciones.

Vemos que el alcance real *indoor* del AP Linksys es de aproximadamente 40 % y del 36 % el AP TrendNet. El alcance *outdoor* llega al 50 % y al 40 % respectivamente. Se hará una evaluación más exacta para determinar los radios de cobertura mediante el cálculo de calidad del enlace.

Con las ubicaciones posibles de los APs mostradas en la **Figura 3.3.** y con la estimación de los radios de cobertura de los APs, no se alcanza cobertura para la zona encerrada en la elipse amarilla. Se hace necesario implementar un *bridge* o un modo WDS⁴ para esta zona. Se implementará la solución con los APs suministrados porque la Universidad así lo quiere, pues quiere seguir con el respaldo y confianza de su habitual distribuidor en cuanto a descuentos, facilidades de pago y soporte tecnológico.

Para el cálculo de calidad del enlace microondas entre el punto de distribución y la estación móvil se tiene la ecuación de Friss de cálculo de potencias en espacio libre:

$$P_{tx} = P_{rx} + L - G$$

Donde: **P_{tx}** = Potencia de transmisión

P_{rx} = Potencia de recepción

L = Pérdidas por atenuación

G = Ganancia de la antena

La potencia máxima de transmisión según el Decreto 0797/ de 2001 de la CRT⁵ no debe exceder de **100 mW o 20 dBm.**

Para el AP Linksys⁶:

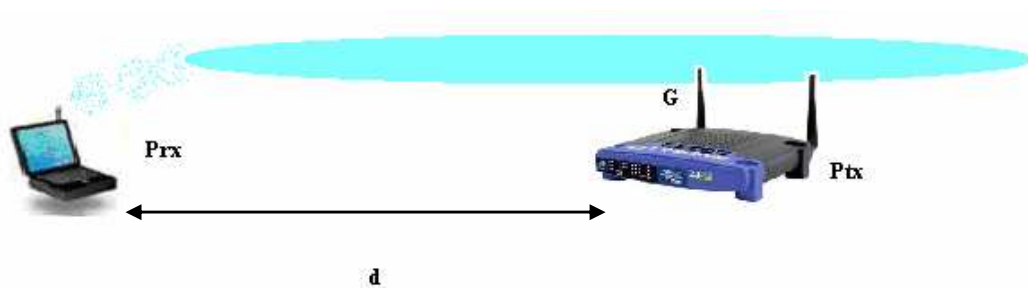


Figura 3.18. Enlace AP Linksys – STA

Potencia de recepción

$$P_{rx}: P_{rx} = S_{rx} + MD$$

Donde: **S_{rx}** = Sensibilidad del receptor

MD = Margen de debilitamiento

⁴ Wireless Distribution System. Sistema de distribución inalámbrico mediante el cual se interconectan varios puntos de acceso. Es un modo de operación *bridge* de los APs. No todos los APs tienen esta característica.

⁵ Comisión de Regulación de las Telecomunicaciones

⁶ Ver Anexo G.

La sensibilidad **Srx** es la potencia de recepción umbral o nivel de señal mínima para que haya comunicación. Esta sensibilidad varía de acuerdo a la tasa de transmisión disminuye.

Según las especificaciones del adaptador PCMCIA TEW 401 PC mostradas en el ANEXO G:

$$S_{rx} = -65 \text{ dBm a } 54 \text{ Mbps}$$

$$S_{rx} = -80 \text{ dBm a } 11 \text{ Mbps}$$

La sensibilidad varía según la tasa de transmisión disminuye.

El margen de debilitamiento **MD** es el nivel de señal recibida por encima del nivel de sensibilidad del receptor, para evitar indisponibilidad del sistema. La siguiente tabla muestra los valores de disponibilidad para calcular el MD, usando el método de Rayleigh⁷. Típicamente el MD está entre 20 y 30 dB.

MD (dB)	Disponibilidad (%)
8	90
18	99
28	99.9
38	99.99
48	99.999

Tabla 3.6. Disponibilidad y desvanecimiento del enlace

Fuente: Referencia [3]

Se quiere una disponibilidad del 99 % así que el MD será de 18 dB.

Entonces, según las especificaciones del adaptador, en el ANEXO G:

$S_{rx} = -65 \text{ dBm a } 54 \text{ Mbps}$, $-67 \text{ dBm a } 48 \text{ Mbps}$, $-70 \text{ dBm a } 36 \text{ Mbps}$, $-75 \text{ dBm a } 24 \text{ Mbps}$, $-78 \text{ dBm a } 18 \text{ Mbps}$, $-82 \text{ a } 12 \text{ Mbps}$, $-85 \text{ dBm a } 9 \text{ Mbps}$, $-89 \text{ dBm a } 6 \text{ Mbps}$.

Eligiendo el peor caso, para una tasa de 6 Mbps:

$$MD = 18 \text{ dB}$$

$$Pr_x = -89 \text{ dBm} + 18 \text{ dB} = -71 \text{ dBm} = -101 \text{ dB}$$

$$Pr_x = -101 \text{ dB}$$

⁷ Lord Rayleigh en 1871 mostró que la luz del sol es dispersada en todas direcciones por las moléculas de aire. De ahí viene esta atenuación que encontró lugar en los efectos de multitrayectoria en técnicas de transmisión inalámbrica de alta frecuencia. Tal como la luz, también las ondas electromagnéticas de alta frecuencia son dispersadas por las moléculas de aire

La ganancia **G** será la ganancia de la antena transmisora del AP y está en las especificaciones:

$$G = 2 \text{ dBi}$$

Las Pérdidas asociadas a la propagación están dadas por:

$$L = L_o + L_{emp} + L_{lt} + L_{obs} + L_{refl}$$

Donde: **L_o** = pérdidas por espacio libre

L_{emp} = pérdidas por empalmes

L_{lt} = pérdidas por línea de transmisión

L_{obs} = pérdidas por obstáculos

L_{refl} = pérdidas por reflexión

La altura promedio de los edificios es de 5 metros, a esta altura se colocarán los APs para disminuir las interferencias de trayectoria y aprovechar el patrón de radiación. Para este caso, debido a las distancias cortas, se obvian las pérdidas por reflexión, además no existen pérdidas por empalmes ni por línea de transmisión.

Tampoco existirán pérdidas por obstáculos pero se tomará el caso de un obstáculo que corresponde a la pared exterior de las edificaciones, de 10 cm de espesor. Para tener una estimación se vale de la siguiente tabla:

OBSTÁCULO	PÈRDIDA (dB)
Espacio libre	0
Ventana	3
Pared fina (madera)	5 a 8
Pared gruesa (aprox. 15 cm)	15 a 20
Pared muy gruesa (aprox. 30 cm)	20 a 25
Piso o techo grueso	15 a 20
Piso o techo muy grueso	20 a 25

Tabla 3.7. Atenuación de potencia por material de construcción

Fuente: Trabajo de Maestría Referencia [6]

Tomando el valor de 8 dB para paredes:

$$L_{obs} = 8 \text{ dB} * 1 = 8 \text{ dB}$$

Para las pérdidas por espacio libre:

$$L_o = 20 \log (4 \cdot \pi \cdot d \cdot f / c)$$

d = distancia entre el transmisor y el receptor

f = frecuencia del canal de transmisión = 2400 MHz o 2.4 GHz

$$c = 3 \cdot 10^8 \text{ m/s}$$

Para frecuencias diferentes a 2.4 GHz se usa la expresión en dB:

$$L_o = 32.4 + 20 \log [d \text{ (Km)}] + 20 \log [f \text{ (MHz)}]$$

Para el canal 1 f1= 2412 MHz, canal 6, f6= 2437 canal 11, f11= 2462, como se explica en el ANEXO C y en la Figura C.4.

Pero cuál debe ser la distancia **d** óptima del usuario móvil al AP?

Tenemos entonces,

$$L = L_o + L_{obs}$$

Ptx = 18 dBm según especificaciones del AP.

$$P_{tx} = P_{rx} + L - G$$

$$P_{tx} + G - P_{rx} - L_{obs} = L_o$$

$$18 \text{ dBm} + 2 \text{ dB} + 101 \text{ dB} - 8 \text{ dB} = 20 \log (4 \cdot \pi \cdot d \cdot f / c)$$

$$113 \text{ dBm} = 83 \text{ dB} = 20 \log (4 \pi d (2400 \cdot 10^6) / 3 \cdot 10^8)$$

$$83/20 = 4.15 = \log (100,5309649 \cdot d)$$

$$10^{4.15} = 100,5309649 \cdot d$$

$$140.5 \text{ m} = d$$

Ahora para la frecuencia f1 = 2412 MHz, se usa la siguiente expresión para Lo:

$$L_o = 32.4 + 20 \log [d \text{ (Km)}] + 20 \log [2412]$$

$$P_{tx} = P_{rx} + L - G$$

$$L = L_o + L_{obs}$$

$$P_{tx} + G - P_{rx} - L_{obs} = L_o$$

$$18 \text{ dBm} + 2 \text{ dB} + 101 \text{ dB} - 8 \text{ dB} = 32.4 + 20 \log [d \text{ (Km)}] + 20 \log [(2412)]$$

$$18 \text{ dBm} + 2 \text{ dB} + 101 \text{ dB} - 8 \text{ dB} - 32.4 \text{ dB} - 67.64 \text{ dB} = 20 \log [d \text{ (Km)}]$$

$$12.96 \text{ dBm} = (-17.04 \text{ dB}) / 20 = \log [d (\text{Km})]$$

$$10^{-0.852} = d (\text{Km})$$

$$140.6 \text{ m} = d$$

Tomando el mismo procedimiento para diferentes sensibilidades y tasas de transmisión y para los canales 1, 6 y 11 se obtiene la siguiente tabla:

Sensibilidad en dB	Tasa de transmisión en Mbps	f = 2400 MHz	Canal 1 f = 2412 MHz	Canal 6 f = 2437 MHz	Canal 11 f = 2462 MHz
-65	54	8.8 m	8.86 m	8.73 m	8.64 m
-67	48	11.16 m	11.15 m	10.99 m	10.87 m
-70	36	15.75m	15.68 m	15.62 m	15.36 m
-75	24	28.03 m	27.89 m	27.60 m	27.32 m
-78	18	39.6 m	39.40 m	38.99 m	38.60 m
-82	12	62.76 m	62.45 m	61.80 m	61.18 m
-85	9	88.65 m	88.21 m	87.30 m	86.42m
-89	6	140.5 m	140.6 m	138.37 m	136.96 m

Tabla 3.8. Distancias óptimas de STA al AP Linksys

Para el AP TrendNet⁸:

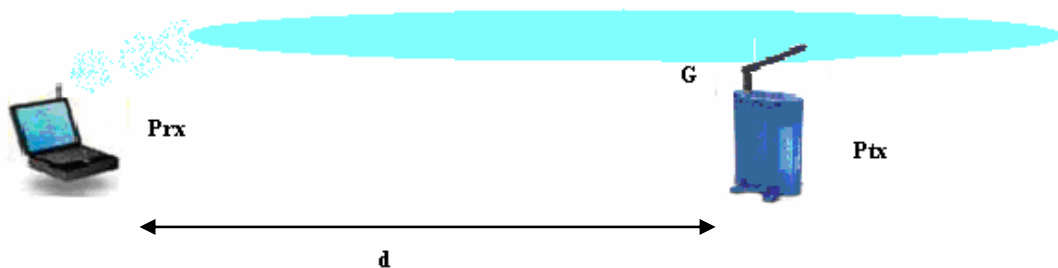


Figura 3.19. Enlace AP TrendNet - STA

$$P_{tx} = 15 \text{ dBm}$$

$$G = 2 \text{ dBi}$$

$$S_{rx} = -65 \text{ dBm a } 54 \text{ Mbps}$$

⁸ Ver Anexo G.

$$S_{rx} = -80 \text{ dBm a } 11 \text{ Mbps}$$

$$MD = 18 \text{ dB}$$

$$Prx = -89 \text{ dBm} + 18 \text{ dB} = -71 \text{ dBm} = -101 \text{ dB} \quad \mathbf{Prx = -101 \text{ dB}}$$

Pérdidas: $L = L_o + L_{obs}$

$$P_{tx} = Prx + L - G$$

$$P_{tx} + G - Prx - L_{obs} = L_o$$

$$15 \text{ dBm} + 2 \text{ dB} + 101 \text{ dB} - 8 \text{ dB} = 20 \log(4 \cdot \pi \cdot d \cdot f / c)$$

$$110 \text{ dBm} = 80 \text{ dB} = 20 \log(4 \pi d (2400 \cdot 10^6) / 3 \cdot 10^8)$$

$$80/20 = 4 = \log(100,5309649 \cdot d)$$

$$10^4 = 100,5309649 \cdot d$$

$$\mathbf{99.47 \text{ m} = d}$$

Sensibilidad en dB	Tasa de transmisión en Mbps	f = 2400 MHz	Canal 1 f = 2412 MHz	Canal 6 f = 2437 MHz	Canal 11 f = 2462 MHz
-65	54	6.65 m	6.27 m	6.21 m	6.14 m
-67	48	7.9 m	7.89 m	7.81 m	7.73 m
-70	36	11.16 m	11.15 m	11.04 m	10.93m
-75	24	19.84 m	19.84 m	19.64 m	19.44 m
-78	18	28.03 m	28.029 m	27.74 m	27.42 m
-82	12	44.43 m	44.42 m	43.96 m	43.52 m
-85	9	62.76 m	62.75 m	62.10 m	61.47m
-89	6	99.47 m	99.46 m	98.43 m	97.43 m

Tabla 3.9. Distancias óptimas de STA al AP TrendNet

Las distancias a las que puede estar un usuario móvil del punto de distribución, en este caso los APs y sin perder conectividad son de 140 metros y 99 metros aproximadamente, aunque a las tasas de transmisión más bajas. El objetivo es tener acceso y cobertura a las mejores tasas de transmisión. El AP Linksys opera al 40 % de su valor nominal y el AP TrendNet al 33 %. Las mediciones muestran que un usuario móvil puede estar a más de 40 metros del AP con una tasa de transmisión superior a los 11 Mbps del 802.11b. Con esto y con las mediciones preliminares de la cobertura *indoor* y *outdoor* tomando un radio de cobertura de 90 metros se lograría conectividad en casi todo el campus con pocos APs pero a tasas de transmisión bajas. Para mejorar esto se tomará 40 metros para el AP Linksys y 35 metros para el AP TrendNet como radios de cobertura, para asegurar transmisiones mínimas de 18 Mbps. Se tomarán ubicaciones para los APs cada 60 o 70

metros, pues el traslape de los APs debe ser de 10 a 15 % para asegurar roaming. En las tablas anteriores la elección del canal no tiene una incidencia tan marcada en la cobertura, sin embargo para frecuencias mayores o menores longitudes de onda las pérdidas son mayores y por ende las tasas de transmisión menores. El alcance de las ondas está limitado a las atenuaciones que sufre la señal a medida que se alejan de las fuentes que las generaron.

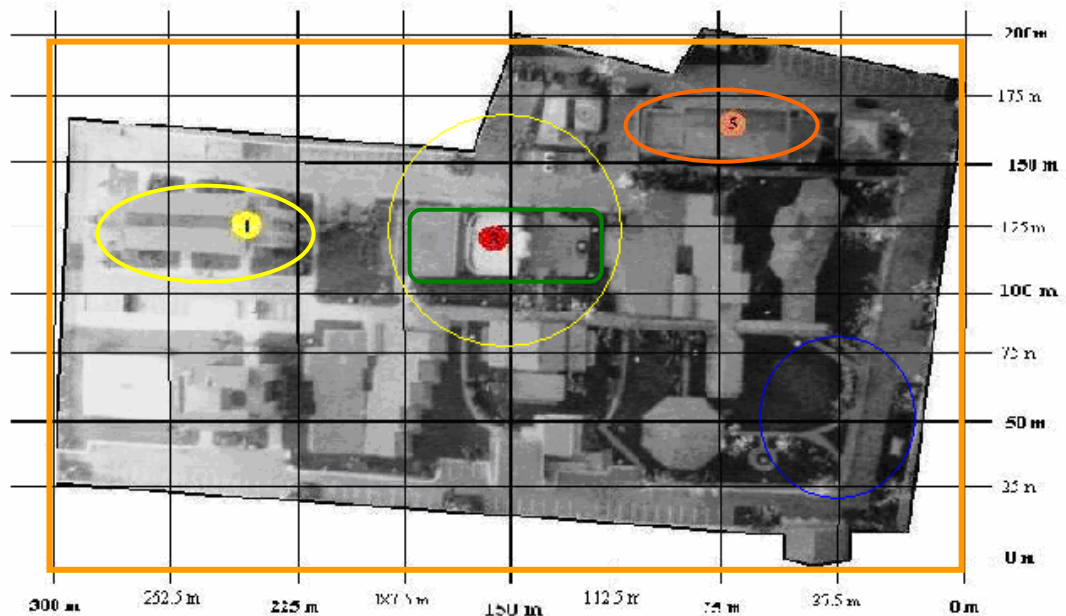


Figura 3.20. División espacial UNIAGRARIA

En la maqueta se hizo una cuadrícula para dimensionar las diferentes distancias y los radios de cobertura para los APs. En la **Figura 3.20.** se muestra el campus dividido en cuadros y los radios de cobertura, en color amarillo el radio de 40 m para el AP Linksys y en color azul el radio aproximado de 35 m para el AP TrendNet. Los mayoristas y distribuidores de productos Cisco ofrecen sus APs con un radio de cobertura de 45 metros (aproximadamente 150 pies). Generalmente los APs en ambientes *indoor* soportan alcances entre 45 y 60 metros.

Pero cuál es el número de APs necesarios?

Existe una metodología propuesta por Cisco Systems en la cual se relaciona el radio de cobertura en función del tipo de edificaciones y de los requerimientos promedio de desempeño de los usuarios.

El factor Z es la longitud del cuadrado o área, que representa la cobertura del AP.

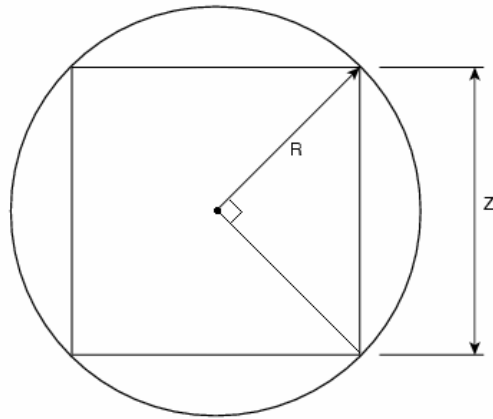


Figura 3.21. Cobertura Factor Z

$$Z = \sqrt{R^2 + R^2}$$

La relación para saber el número de APs consiste en dividir el área de trabajo en rectángulos y el área de estos dividirla por el factor Z. Las áreas de cobertura deseadas se muestran en la **Figura 3.10.** y en la **Figura 3.18.** se considera toda el área de la universidad como un solo rectángulo en color naranja, por las características comunes de la señal RF a través de las edificaciones debido a la homogeneidad de la arquitectura.

$$\text{APs} = \text{Área rectángulos} / Z$$

Se dijo que el área aproximada de UNIAGRARIA es de 200 m x 300 m = 60000 m²

Para el AP Linksys R = 40 m Z = 57

$$\text{Área cobertura } Z^2 = 3249 \text{ m}^2$$

$$\text{APs} = (200/57) * (300/57)$$

$$\text{APs} = 18 \text{ APs}$$

Para el AP TrendNet R = 35 m Z = 50

$$\text{Área cobertura } Z^2 = 2500 \text{ m}^2$$

$$\text{APs} = (200/43) * (300/43)$$

$$\text{APs} = 24 \text{ APs}$$

Esto nos da una estimación para lograr una cobertura del 100 % del campus. En un área de (Lado 1)*(Lado 2) como en la **Figura 3.20.** la 'X' representa la ubicación del AP y hay que notar que el Factor Z es el mismo entre los centros de los APs y los cuadrados en color verde cuando los cuadrados están adyacentes.

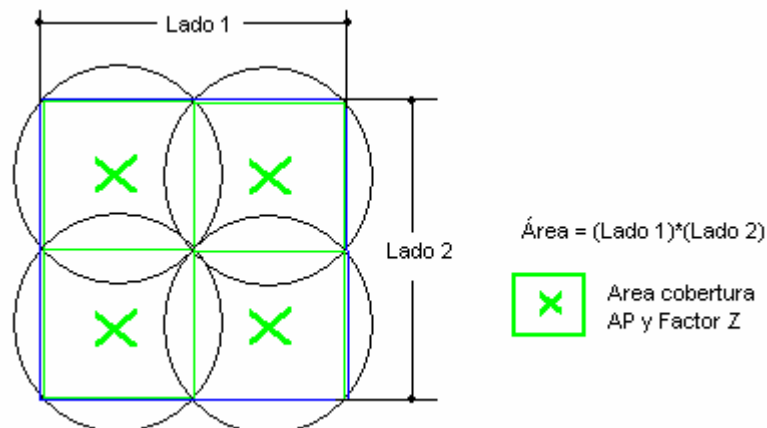


Figura 3.22. Ubicación APs según Factor Z

Como se quiere un cubrimiento del 90 % seguramente el número de APs será menor, siendo entonces la reducción del número de APs un objetivo de diseño, además este tipo de ubicaciones no tienen en cuenta las facilidades de la red de datos y la red eléctrica lo que aumentaría costos adicionales de implementación en cableado eléctrico y cableado lógico.

Como se mencionó es necesario realizar una implementación en modo WDS para la zona del edificio marcado con el número uno y determinar zonas de Fresnell. El modo WDS a usar será el modo *Repeater* o modo repetidor.

Existen cuatro posibles puntos desde donde implementar el WDS, el punto de Sistemas 3, biblioteca, ingenierías o deportes. Se tomará desde deportes pues es la distancia mas corta para tener una mejor calidad del enlace.

La ecuación de Fresnell:

$$r1 = \sqrt{\frac{\lambda \cdot n1 \cdot d1 \cdot d2}{d1 + d2}}$$

r1 = radio de la zona de Fresnell

λ = longitud de onda

d = d1 + d2

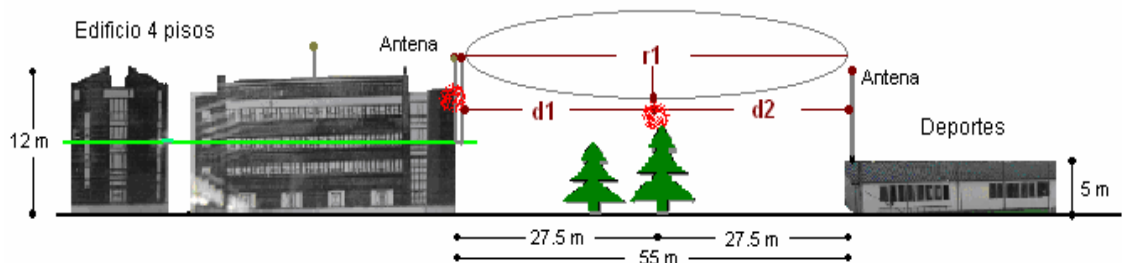


Figura 3.23. Zona de Fresnell para WDS

d = 55 m

d1 = 13 m

d2 = 42 m

Altura Edificio 4 pisos = 12 m Altura Deportes = 5 m Altura obstáculos = 5 m

La determinación de r1 sirve para establecer la altura de las antenas a partir de una referencia. Se puede obviar el efecto de 'fading' o de la curvatura terrestre. Los puntos más críticos están marcados con rojo en la **Figura 3.23**, que corresponden al edificio de 4 pisos y al punto medio del enlace. Hay unos árboles como obstáculos de 5 metros de altura entre el edificio de 4 pisos y Deportes.

La altura de referencia para la transmisión en Deportes es de 5 metros y la altura de referencia de la antena de recepción en el edificio de 4 pisos es el punto medio de este que es de 6 metros. La antena se colocará en la fachada sur a la altura del segundo piso, para brindar cobertura a los pisos inferiores y superiores y facilitar un posible incremento e implementación de equipos de red y subredes a partir de este punto de distribución.

$$c = \lambda * f$$

$$\lambda = c / f$$

$$\lambda = 3 * 10^8 \text{ m/s} / 2400 * 10^6 \text{ s}^{-1}$$

$$\lambda = 125 \text{ mm} = 0.125 \text{ m}$$

Asumiendo para la primera zona de Fresnell $n1 = 1$:

Para el primer punto crítico (borde fachada sur):

$$d1 = 13 \text{ m}$$

$$d2 = 42 \text{ m}$$

$$r1 = \sqrt{\frac{(0.125)(13)(42)}{13 + 42}}$$

$$r1 = 1.11 \text{ m}$$

$r1 = 1.11$ metros me quiere decir que para este punto las antenas se deben colocar 1.11 metros por encima de la altura de referencia. Para este punto la antena estará entonces a una altura de 7.11 metros.

Para el punto medio del enlace:

$$d1 = 27.5 \text{ m}$$

$$d2 = 27.5 \text{ m}$$

$$r1 = \sqrt{\frac{(0.125)(27.5)(27.5)}{13 + 42}}$$

$$r1 = 1.31 \text{ m}$$

La antena estará a 1.31 metros de la referencia, es decir a 6.31 metros.

Estas son las alturas a las cuales se ubicarán las antenas para garantizar una condición de visibilidad libre de obstáculos, en estas regiones de 1.11 metros y 1.31 metros se concentrará el 90 % de la energía electromagnética.

Para el cálculo del enlace:

$$P_{tx} = P_{rx} + L - G$$

$$G = G_{tx} + G_{rx}$$

G_{tx} = Ganancia antena transmisora

G_{rx} = Ganancia antena receptora

Para la transmisión se utilizará el AP WRT54G de Linksys y para la recepción una AP TEW 432 BRP de TrendNet. Se usarán antenas omnidireccional referencia TEW OA080 de TrendNet de ganancia 8 dBi, impedancia de 50 Ω y potencia de 50 W.⁹

Para G entonces:

$$G_{tx} = G_{rx} = 8 \text{ dBi}$$

$$G = 8 \text{ dBi} + 8 \text{ dBi} = 16 \text{ dBi}$$

Pérdidas:

$$L = L_o + L_{emp} + L_{lt} + L_{obs} + L_{refl}$$

Donde: L_o = pérdidas por espacio libre

L_{emp} = pérdidas por empalmes y conectores

⁹ Ver Anexo G.

Llt = pérdidas por línea de transmisión

Lobs = pérdidas por obstáculos

Lrefl = pérdidas por reflexión

Como las zonas de Fresnell deben estar libres de obstáculos, las pérdidas Lobs y Lrefl se omiten.

Para Lemp, en microondas las pérdidas por empalmes son típicamente de 0.1 dB y las pérdidas debido a conectores son de 0.5 dB. En cada lado del WDS están los conectores que unen el AP con la antena, AP-cable y cable-antena. Así se tienen cuatro conectores:

$$Lemp = 4 * 0.5 \text{ dB} = 2 \text{ dB}$$

Las pérdidas Llt, usando cable coaxial LMR-400 referencia TEW 406 de TrendNet para la conexión de las antenas a los APs. Entonces para la transmisión en Deportes la distancia de la antena será de 1.31 metros desde la referencia, esta será la distancia del cable desde el AP hasta la antena. Para la recepción es de 1.11 metros. Este cable introduce unas pérdidas de 22 dB/100m.

Para 1.31 m: $Llt = (0.22 \text{ dB/m}) * 1.31 \text{ m} = 0.288 \text{ dB}$

Para 1.11 m: $Llt = (0.22 \text{ dB/m}) * 1.11 \text{ m} = 0.24 \text{ dB}$

$$Llt = 0.288 \text{ dB} + 0.24 \text{ dB} = 0.53 \text{ dB}$$

Ahora Lo,

$$Lo = 20 \log (4.\pi.d.f / c)$$

$$Lo = 20 \log (4.\pi.55.2400 * 10^6 / 3 * 10^8)$$

$$Lo = 74.85 \text{ dB}$$

Se obtiene lo mismo con: **Lo = 32.4 + 20log [d (Km)] + 20log [(2400)]**

$$Lo = 32.4 + 20 \log [0.055] + 20 \log [2400]$$

$$Lo = 74.81 \text{ dB}$$

$$L = 2 \text{ dB} + 0.53 \text{ dB} + 74.8 \text{ dB}$$

$$L = 77.33 \text{ dB}$$

$$Ptx + G = Prx + L$$

$$Ptx = 18 \text{ dB para WRT54G}$$

$$Ptx + G - L = Prx$$

$$18 \text{ dB} + 16 \text{ dB} - 74.81 \text{ dB} = -40.81 \text{ dB} = Prx$$

$$Prx = S + MD \quad MD: 28 \text{ dB para } 99.9 \%$$

$$S = Prx - MD$$

$$S = -40.81 \text{ dB} - 28 \text{ dB} = -68.81 \text{ dB}$$

Quiere decir que el enlace estará disponible un 99.9 % y según la especificaciones del AP a una tasa mínima de 36 Mbps para esta sensibilidad.

Con estas consideraciones, se empezará a determinar las ubicaciones de los APs desde el centro del campus hacia fuera separados aproximadamente entre 60 y 70 metros. El centro del campus es la Biblioteca, el siguiente AP a ubicar será el de Deportes desde donde se hará el modo WDS. Se continúa así ‘de adentro hacia fuera’ hasta llegar al perímetro de la universidad, cuidando que haya traslape de los rangos de cobertura. Se combina la solución con ambos rangos de cobertura, el del AP Linksys y el del AP TrendNet, para reducir el número de APs a utilizar y evitar zonas de cubrimiento indeseadas por fuera del campus. La ubicación preliminar de los APs y la distribución de canales, como lo explica el ANEXO C, teniendo en cuenta lo anterior en la siguiente figura:

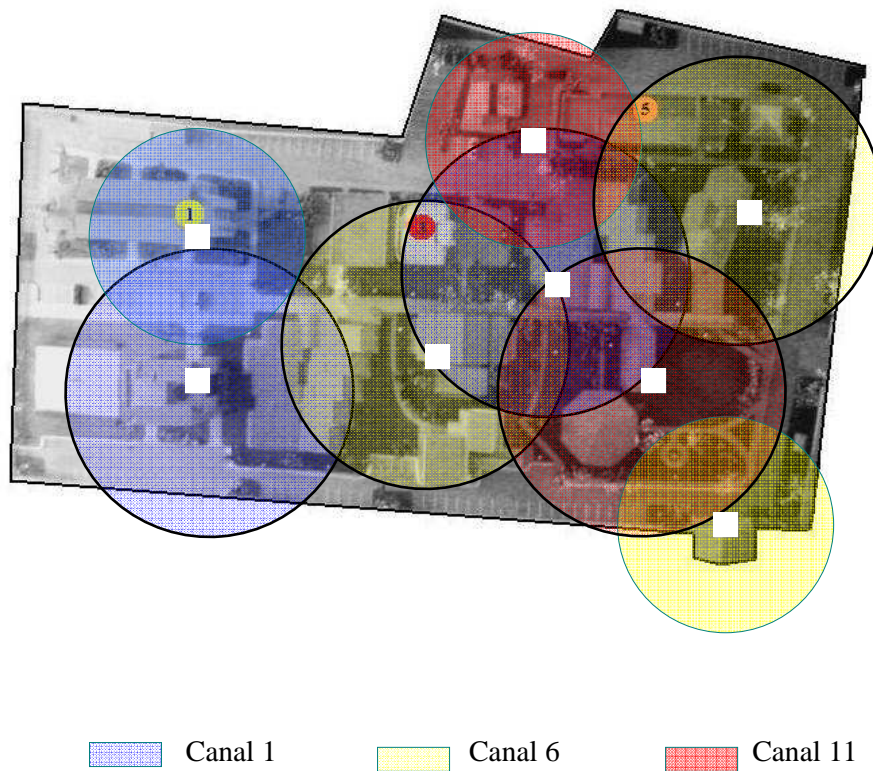


Figura 3.24. Ubicación APs

Biblioteca	AP Linksys	Canal 6
Deportes	AP Linksys	Canal 1
Asist. Sistemas/Sala Internet	AP Linksys	Canal 1
Derecho	AP Linksys	Canal 11
Bienestar	AP TrendNet	Canal 6
Oficinas Profesores	AP TrendNet	Canal 11
Consejo Superior	AP TrendNet	Canal 1
Edificio 4 Pisos	AP BRP TrendNet	Canal 1 – WDS

Se obtuvo un total de 8 APs reduciendo considerablemente la estimación teórica de 18 APs.

- **Verificación de la ubicación de los AP.**

Para la verificación de las ubicaciones se uso el monitor de red inalámbrica NetStumbler, y el generador de tráfico Qcheck como *site survey tools*. Ambas herramientas son de distribución libre. NetStumbler me permite detectar APs u otras redes inalámbricas presentes, interferencias, fuerza de la señal, SNR, ruido, direcciones IP, SSID, encriptación. Check genera tráfico TCP, UDP, SPX, permite simular transmisiones de video y audio. Las siguientes figuras muestran ejemplos de las interfaces gráficas de estas herramientas:



Figura 3.25 (a). Consola Check

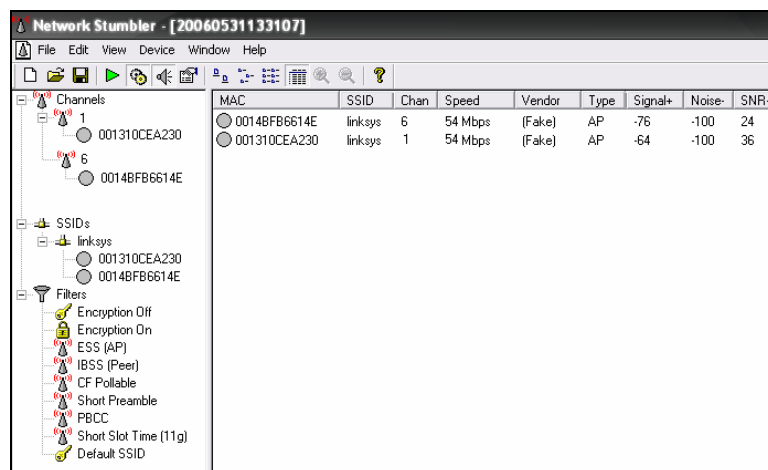


Figura 3.25 (b). Consola NetStumbler

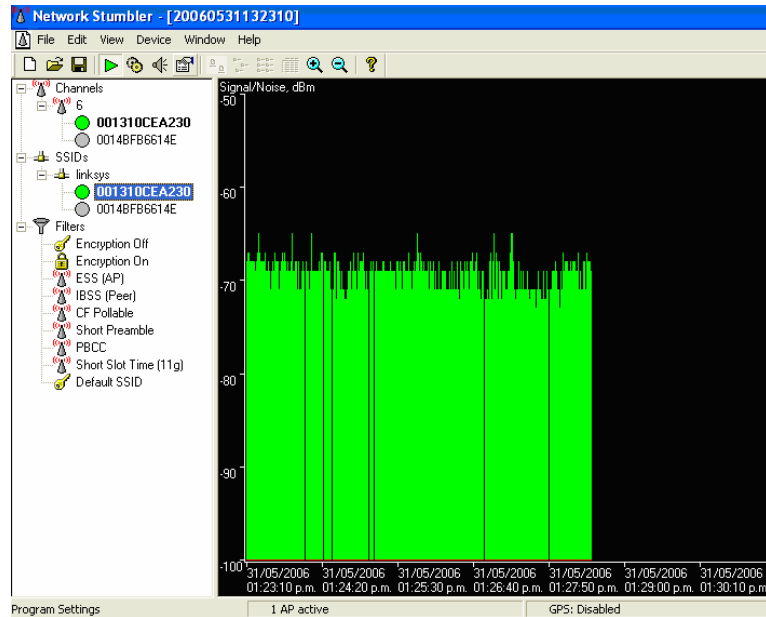


Figura 3.25 (c). Consola NetStumbler

Se quiere caracterizar como se comporta la señal RF y como se comporta la tasa de throughput en diferentes ubicaciones del AP.

Con la herramienta QCheck se generó tráfico TCP con tamaño de paquetes de 1500 bytes para registrar la tasa efectiva de throughput y con el monitor NetStumbler se registró la fuerza de la señal en dBm para diferentes ubicaciones de la estación móvil.

Las tasas promedio teóricas de throughput esperadas para enlaces inalámbricos son:

Estándar	Modulación	Velocidad de transferencia Máxima	Máxima tasa TCP	Máxima tasa UDP
802.11g	OFDM / CCK	54 Mbps	24.4 Mbps	30.5 Mbps
802.11b	CCK	11 Mbps	5.9 Mbps	7.1 Mbps
802.11g 11b	y OFDM / CCK	54 Mbps	14.4 Mbps	19.5 Mbps

Tabla 3.10. Máximos teóricos throughput

Fuente: Referencia [3]

Para la primera prueba se usó un AP Linksys WRT54G ubicado en Asistencia sistemas/sala Internet en la esquina nor-occidental del edificio, con las siguientes ubicaciones, y especial interés en posiciones como la 4, 6, 7, 8, 9 y 10 donde la celda se traslapará con otra celda adyacente:

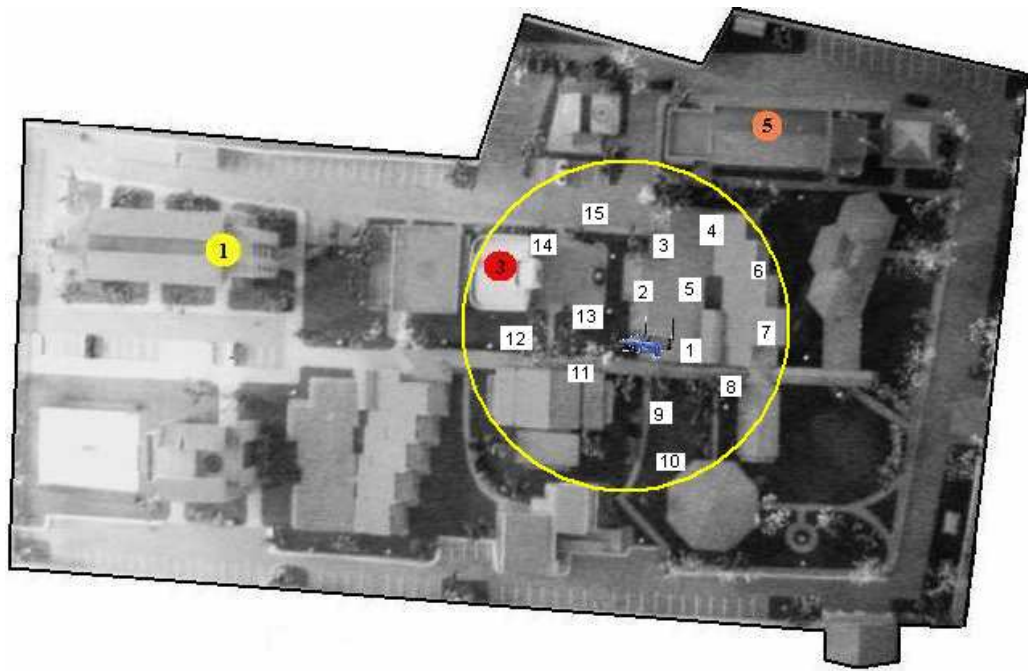


Figura 3.26. Verificación AP Linksys sistemas/sala Internet

Punto medida	Distancia [m]	Señal [dBm]	Throughput [Mbps]
1	10	-58	22.4
2	11	-61	20.3
3	25	-65	14.3
4	27	-64	16.2
5	19	-62	18.3
6	37.5	-60	14
7	40	-74	2.7
8	38	-61	14
9	26	-59	16.2
10	38	-70	7.3
11	16	-63	16.8
12	36	-74	3.9
13	18	-68	11
14	38.5	-66	13.5
15	39	-72.5	4.01

Tabla 3.11. Prueba1 AP Linksys sistemas/sala Internet

El promedio de throughput es de 11.77 Mbps

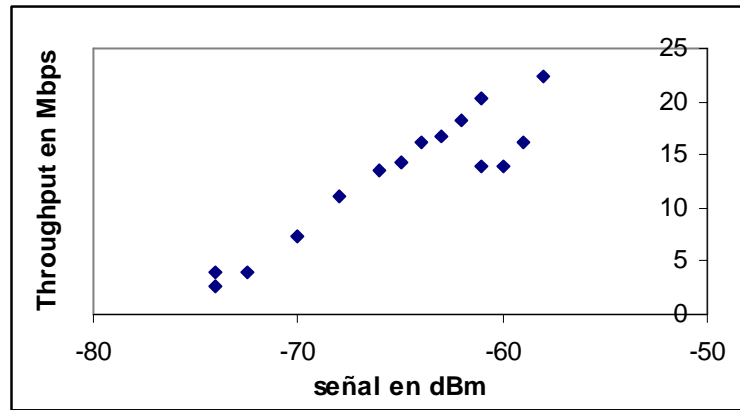


Figura 3.27. Throughput vs. Fuerza de la señal prueba1

En la segunda prueba se ubicó el mismo AP Linksys en Biblioteca, en la esquina nor-occidental.

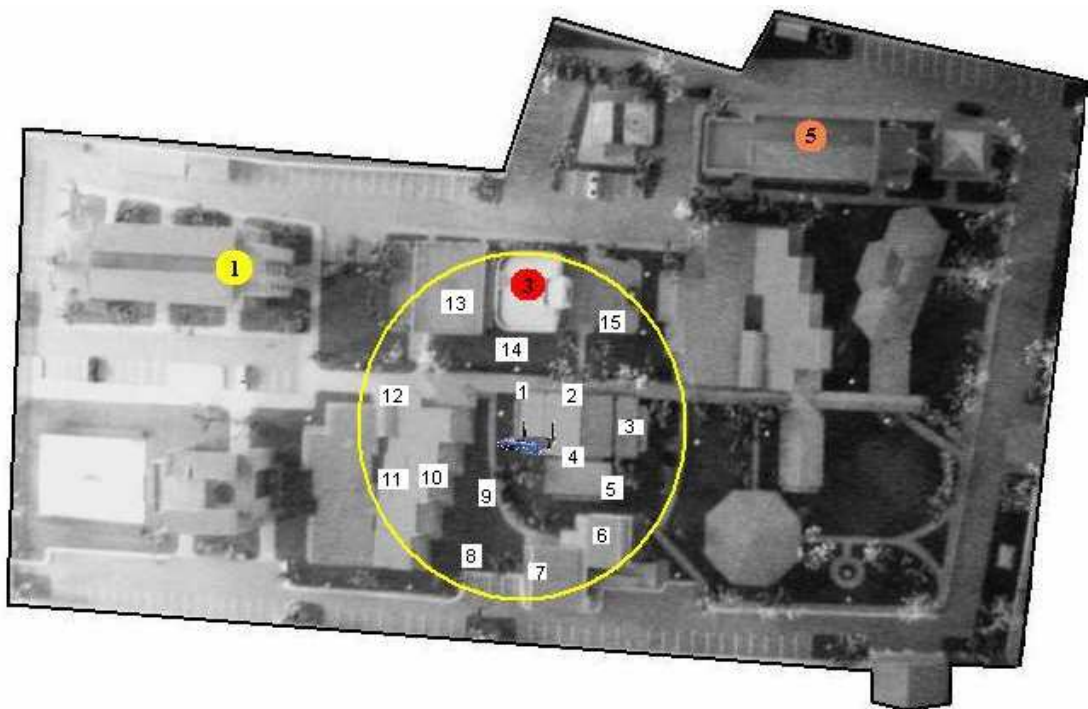


Figura 3.28. Verificación AP Linksys Biblioteca

Punto medida	Distancia [m]	Señal [dBm]	Throughput [Mbps]
1	5	-56	21.4
2	10	-59	17.2
3	20	-65	14.4
4	8	-64	15.9
5	25	-65	14.3
6	31	-66	13
7	37	-70	4.41
8	38	-72	4.1
9	19	-63	15.2
10	37.5	-64	12.8
11	39	-75	2.35
12	39.4	-74	3.85
13	38	-69	6.57
14	30	-64	13
15	40	-67	6.1

Tabla 3.12. Prueba2 AP Linksys Biblioteca

El promedio de throughput es de 10.97 Mbps.

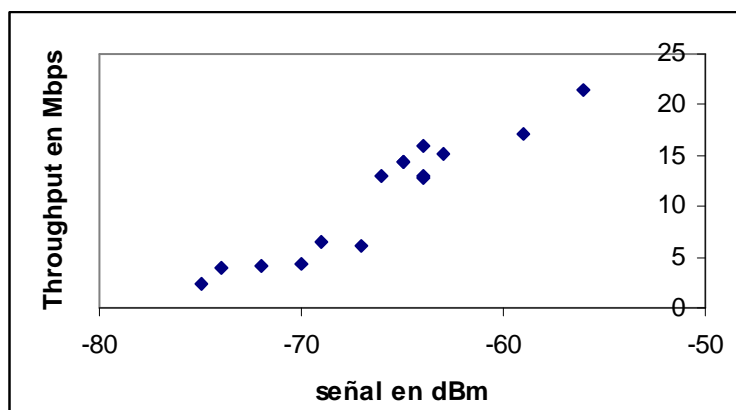


Figura 3.29. Throughput vs. Fuerza de la señal prueba2

Para la última prueba se ubicó el AP Linksys en Deportes y el TrendNet 423 BRP configurados en modo WDS repetidor, para estimar el desempeño. Ambos APs comparten el canal 1 de 2412 MHz. A partir de la posición 15 la distancia se tomó con referencia al AP en modo WDS.

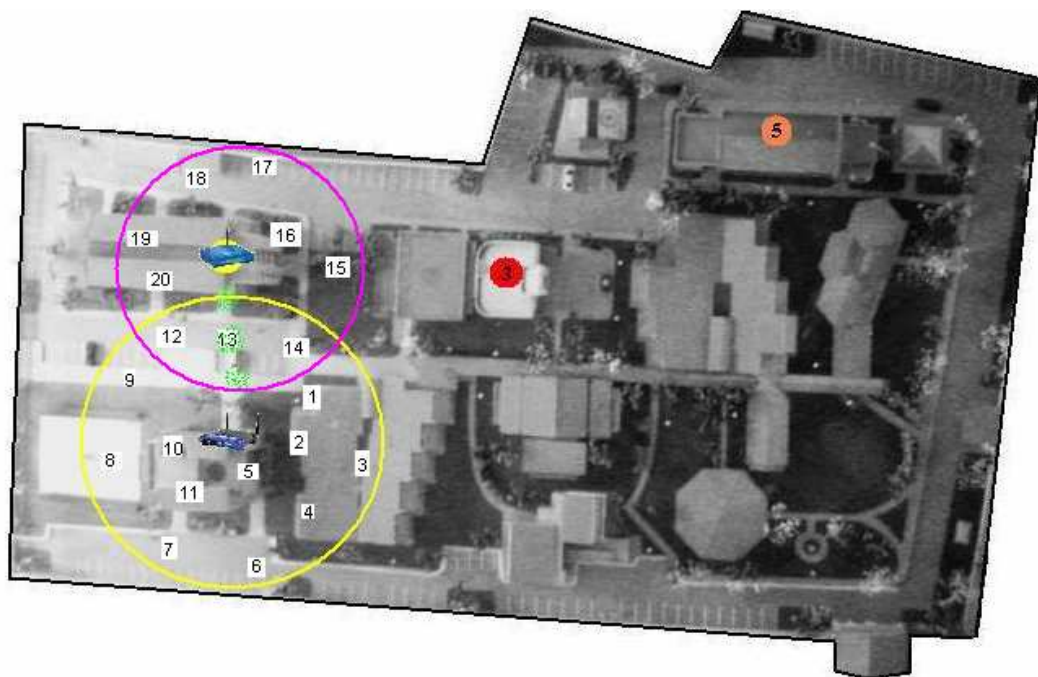


Figura 3.30. Verificación AP Linksys WDS

Punto medida	Distancia [m]	Señal [dBm]	Throughput [Mbps]
1	24	-65	11.3
2	12	-62	12
3	39	-70	7.6
4	27	-69	9.3
5	10	-64	10.3
6	39	-59	4.7
7	37	-57	3.7
8	38.5	-55	2.2
9	39.5	-51	1.8
10	13	-71	7.5
11	22	-73	6.2
12	37	-74	2.6
13	35	-69	2.9
14	38	-66	3.3
15	34	-65	2.6
16	14	-69	4.8
17	35	-75	1.5
18	34	-74	1.3
19	33	-75	1.2
20	31.5	-72	1.8

Tabla 3.13. Prueba3 AP Deportes modo WDS

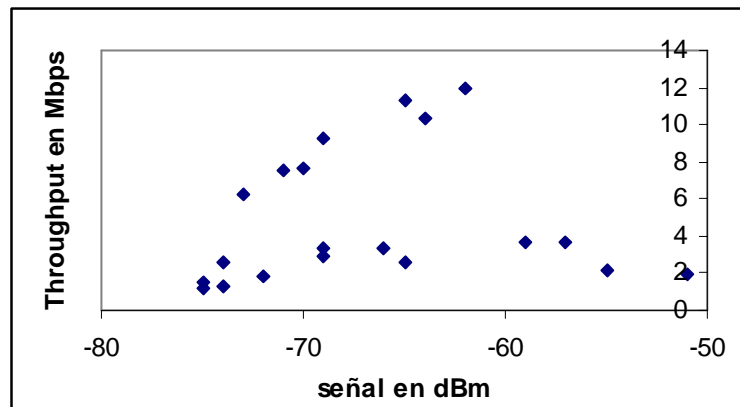


Figura 3.31. Throughput vs. Fuerza de la señal prueba3

El promedio para el AP Linksys tomando las primeras 14 posiciones es de 6.1 Mbps y para el AP TrendNet WDS desde la posición 12 es de 2.12 Mbps.

El promedio del throughput está relacionado con el estándar 802.11 y con la fuerza de la señal. A más fuerza de la señal mayor throughput. Sin embargo hay un punto en el cuál la mayor fuerza de la señal no aumenta el throughput promedio. Según los resultados de las gráficas el throughput empieza a mejorar en el rango de - 75 dBm y - 55 dBm. EL modo WDS decrementa la tasa de throughput debido a que debe transmitir en el mismo canal, así cuando un AP envía, el otro no puede enviar o recibir.

Los promedios obtenidos de desempeño de throughput son menores que los nominales casi en la mitad, para la tasa de transmisión de 54 Mbps se espera un valor de throughput nominal de 24.4 Mbps, como se diseño para tasas mínimas de transmisión de 18 Mbps se esperaban tasas throughput del orden de 9Mbps y se tienen tasas promedio 11.97 y 10.97 Mbps, lo cual indica un buen desempeño. Para el enlace WDS las verificaciones indican que la sensibilidad calculada puede ser mayor y la tasa throughput estará para transmisiones mínimas de 12 y 18 Mbps.

• Documentación

Las especificaciones y esquemas finales de diseño quedan así:

El modo de operación será modo infraestructura, en la aplicación de ampliación de red LAN. Los puntos de acceso serán configurados en modo AP y habrá un modo de operación WDS como repetidor para la zona del edificio de 4 pisos. Se tendrá tasa de transmisión nominal de 54 Mbps y de 18 Mbps mínima, tasa promedio de throughput de 11 Mbps, utilizando dispositivos 802.11g que son compatibles con 802.11b.

Topología física:

Cumpliendo con una cobertura inalámbrica del 90% del campus, disponibilidad del enlace del 99%, incluyendo áreas de descanso, interiores y exteriores y sin brindar cobertura a particulares al exterior de la universidad y sin riesgos de colapsar la red de datos existente, como se muestra en la siguiente figura, se utilizarán los siguientes dispositivos así:

- 5 APs Linksys WRT54G
- 2 APs TrendNet TEW 430 APB
- 1 AP TrendNet TEW 432 BRP
- 2 Antenas Omnidireccionales TrendNet TEW AO080
- Cable LMR-400 TEW 406

Los APs se ubicarán en zonas altas de los edificios, específicamente a la altura del techo dependiendo de la edificación. Y se conectarán a cada switch de borde mediante cable UTP CAT 5E marca AMP.

La caída de algún AP no ocasionará la caída de la red, además el usuario móvil tiene la posibilidad de conectarse a otra celda aledaña.

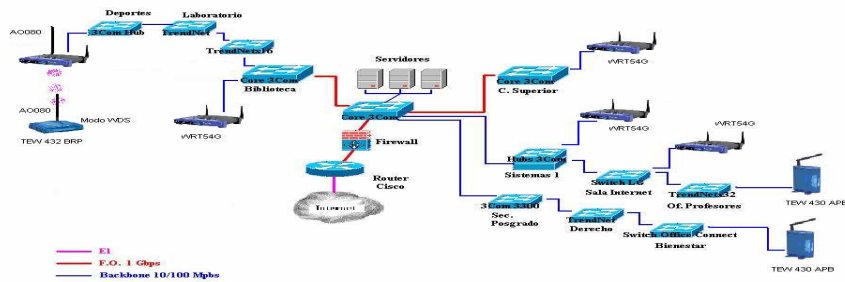


Figura 3.32. Esquema red inalámbrica UNIAGRARIA
Fuente: Autor

Topología lógica:

El direccionamiento de la red de datos es clase C, y la dirección IP para cada AP la da el switch edge o de borde a donde está conectado.

AP	Canal	SSID	WEP	Dirección IP
Linksys WRT54G	6	UNIAG_Biblio	64 bits	DHCP
Linksys WRT54G	1	UNIAG_Sis	64 bits	DHCP
Linksys WRT54G	11	UNIAG_Der	64 bits	DHCP
Linksys WRT54G	1	UNIAG_C.Sup	128 bits	DHCP
Linksys WRT54G	1	UNIAG_Dep	DISABLE	DHCP
TEW 430 APB	11	UNIAG_Prof	128 bits	DHCP
TEW 430 APB	6	UNIAG_Bien	64 bits	DHCP
TEW 432 BRP	1	UNIAG_Dep	DISABLE	DHCP

Tabla 3.14. Equipos a utilizar

El AP con SSID UNIAG_C.Sup tendrá encriptación WEP a 128 bit y filtrado de direcciones MAC, pues este AP brindaría acceso a dependencias como Rectoría y Contabilidad.

Los costos de implementación y de dispositivos inalámbricos están discriminados como sigue en la siguiente Tabla.

Los valores de los dispositivos inalámbricos tienen un precio de distribuidor, que es el precio de costo para la empresa y un precio de utilidad, para estimar así el costo del proyecto tanto para PRESING LTDA. como para UNIAGRARIA. Se mostrarán los precios de utilidad.

Estos precios están sujetos a las variaciones diarias de la Tasa Representativa del Mercado TRM en dólares.

REF.	Cant.	MARCA	Descripción	V/Unitario	V/Total
EQUIPOS WIRELESS					
TEW-430 APB	2	TrendNet.	AP Wireless 802.11g/b 54 Mbps	270,000	540.000
TEW 432 BRP	1	TrendNet.	AP Wireless Router 802.11g/b	350.000	350.000
TEW AO080	2	TrendNet	Antena Omnidireccional 8 dBi	187.500	375.000
TEW 406	1	TrendNet	Cable LMR 400	100.000	100.000
TEW 401 PC	3	TrendNet	Tarjeta adaptador wireless	110.000	330.000
WRT54G	5	Linksys	AP Wireless 802.11g/b	300.000	1'500.000
			CONFIGURACION-PRUEBAS	1'000.000	1'000.000
			Subtotal=		4,195,000
			IVA =	16.00%	671,200
			Total incluido IVA =		4,866,200

Tabla 3.15. Costos estimados

4. CONCLUSIONES Y RECOMENDACIONES

Se presenta un diseño de la red inalámbrica para UNIAGRARIA que brinda cobertura del 90 % del campus a tasas mínimas de transmisión de 18 Mbps, sin generar colisiones ni caídas de servicio. Como criterios para el rango de cobertura se usó variables como el RSSI y la tasa de throughput teniendo en cuenta características *indoor* y *outdoor* y variables como la distancia, pérdidas multirrayectos, obstáculos, tipo de edificación.

Se expresa un procedimiento para llegar a una satisfactoria solución inalámbrica con el fin de enfatizar y dar importancia a la correcta Planeación con el Método de Estudio de Sitio (*Site Survey*) como herramienta veraz y eficiente en la obtención de sistemas óptimos.

Se encontró que la mayoría de implementaciones inalámbricas instaladas no tienen en cuenta la cobertura real y no se aprovecha al máximo los recursos existentes, pues basados en los bajos costos de los dispositivos simplemente se instalan acudiendo a la experiencia, a la intuición y la suposición, resultando en sistemas saturados o ineficientes y de poca cobertura. En la Universidad había un AP conectado a un hub en Sala de Profesores, mal configurado y con pésima cobertura ya que no daba acceso ni la tercera parte de los 23 docentes.

La red de datos de UNIAGRARIA está demasiado segmentada, tiene hubs apilados de 16 puertos a los cuales se conectan switches de 16 puertos y los switches core 3Com de la familia 4200 no tienen la configuración adecuada, esto disminuye el desempeño y no se trabaja a la real capacidad.

El desarrollo de este diseño representa un aporte significativo para PRESING Ltda. en futuras gestiones de diseño y planeación de soluciones inalámbricas.

El throughput depende fuertemente del medio, incluyendo la distancia entre el AP y el STA. Generalmente el throughput decae a medida que la distancia aumenta, pero se tienen distancias cortas con menor tasa de transmisión efectiva, que distancias largas. Un ejemplo fue el caso para las ubicaciones 3, 4 y 9 con distancias de 25, 27, 26 metros y con throughput de 14.3, 16.2 y 16.2 Mbps respectivamente; en la primera prueba de verificación.

Como recomendación para lograr la real capacidad de la red de datos de la Universidad, es necesario reemplazar los hubs existentes por switches de borde de 24 puertos mínimo con funcionalidades de capa 2, 3 y 4, esto pensando en el crecimiento de la red de datos.

También se recomienda hacer un estudio y análisis de tráfico, con el fin de priorizar aplicaciones y dependencias. Aprovechar las potencialidades de los 3Com 4200 como enlaces resilientes, redundancia, QoS, mediante un servicio profesional y certificado de configuración.

Para evitar patrones de radiación que lleguen al exterior del campus se pueden utilizar antenas tipo 'flat' o sectoriales con patrones de irradiación de 95°.

Se puede hacer uso de las herramientas en línea (*On Line Tools*) de compañías como Cisco y 3Com para obtener diseños y sobretodo especificaciones y recomendaciones de equipos inalámbricos de vanguardia en el mercado. Bluetooth ofrece también esta facilidad. Dos de estas *On Line Tools* para diseño y cálculos de potencia se encuentran en:

<http://www.ciscovertools.com/sbnd/index.html> y

<http://tools.cisco.com/cpc/launch.jsp>

Queda abierta la opción de implementar dispositivos 802.11a Turbo con velocidades de transmisión de 108 Mbps así como dispositivos inalámbricos con tecnología Speed Booster. Existe un dispositivo inalámbrico para cada necesidad, o dispositivos inalámbricos con funcionalidades de capas 2, 3 y 4, como enrutamiento, conmutación, firewall, todo en un mismo dispositivo.

Como herramienta alternativa de diseño se puede utilizar software que me permite caracterizar los patrones de radiación y de RSSI en ambientes *indoor* mediante importación o creación de archivos tipo CAD, o una herramienta más sencilla como el OpenWireless diseñado en la UIS. Otras herramientas pueden ser CINDOOR, Winprop, SitePlanner, Net Meter, WebWatchBot, NetflowAnalyzer y/o herramientas propietarias.

REFERENCIA BIBLIOGRAFICAS

- [1] ANSI/IEEE Std 802.11g. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. Estados Unidos: Institute of Electrical and Electronics Engineers, 2003. ISBN 0-7381-3701-4 SS95134.
- [2] ARROYAVE R. Juliana, BRUGUÉS Augusto. Análisis y desarrollo de las tecnologías inalámbricas emergentes y perspectivas dentro de la Universidad de Antioquia. Proyecto de Grado. Dep. Electrónica. Medellín 2004.
- [3] ATHEROS COMMUNICATIONS INC. 802.11 Wireless LAN Performance. Doc. 991-00002-006. Sunnyvale, CA. 2003
- [4] CHEUNG, David y PRETTIE Cliff. A Path Loss Comparison Between the 5 GHz UNII Band (802.11a) and the 2.4 GHz ISM Band (802.11b), Inter Labs, Intel Corporation, Enero 2002.
- [5] DE LUQUE Luis, DÍAZ Irina, VASQUEZ Sandra. Predicción del nivel de intensidad de señal recibid RSSI en una red inalámbrica 802.11b mediante un modelo neuronal. Proyecto de Grado. E3T UIS. Bucaramanga 2005.
- [6] GEIER J. RF Site Survey Steps. Página Web.
- [7] Marcelo Najnudel. “ESTUDO DE PROPAGAÇÃO EM AMBIENTES FECHADOS PARA O PLANEJAMENTO DE WLANS”. Río de Janeiro, Febrero de 2004.
- [8] MINISTERIO DE COMUNICACIONES, Dirección Desarrollo del Sector. Documento informativo de telecomunicaciones proy-res-was 005-dds - 2003. República de Colombia, 2003.
- [9] MINISTERIO DE COMUNICACIONES. Resolución número 3382. Por la cual se autorizan sistemas que operan con tecnología de espectro ensanchado. República de Colombia, 1995.
- [10] PRESING Ltda. Documentos Internos.
- [11] STALLINGS William. Wireless Communications and Networks. Prentice - Hall. Estados Unidos 2002.
- [12] SUÁREZ Martha. LANS inalámbricas: Diseño e implementación de una WLAN para el laboratorio de redes de datos E3T. Proyecto de Grado. E3T UIS. Bucaramanga 2005.
- [13] TANENBAUM Andrew. Redes de Computadores. Pearson Education. México 2003.
- [14] VILLAROEL Carlos, RODRÍGUEZ Angie, VALLE Julio. Diseño de una red de área local inalámbrica. Universidad de Tarapacá Departamento de Electrónica. Arica, Chile 2003.
- [15] YUTACA, Hayacawa. Sistemas de medida wireless LAN y software específico. Revista Española de Electrónica. Barcelona. Marzo de 2003.
- [16] <http://www.amp.co/networking/warranty.html>
- [17] <http://www.cintel.org.com.co>
- [18] <http://www.linksys.com>

- [19] <http://www.trendware.com>
- [20] [http:// www.wi-fi.org](http://www.wi-fi.org)
- [21] <http://www.wi-fiplanet.com/tutorials/article.php/1116311>. 2003

ANEXOS

ANEXO A. TECNOLOGÍA BLUETOOTH

Bluetooth¹⁰ nació en 1994 como una especificación tecnológica desarrollada por Ericsson, entre dispositivos portátiles o dispositivos de escritorio que permitía el intercambio de datos, específicamente para permitir a computadores personales hacer llamadas sobre un teléfono móvil.

Ofrece velocidades de 720 Kbps, así, usando la banda de 2.4 GHz globalmente disponible para usos de baja potencia dos dispositivos Bluetooth pueden compartir hasta 720 Kbps de capacidad separados 10 m el uno del otro.

Esta tecnología está estandarizada bajo la norma 802.15 por la IEEE para desarrollo de redes de área personal (PAN) y las redes inalámbricas de este tipo se denominan WPAN (Wireless PAN).

Los estándares Bluetooth son publicados por un consorcio de la industria conocido como el Bluetooth SIG (Special Interest Group).

El concepto detrás de Bluetooth es proveer una capacidad inalámbrica universal de rango-corto y baja potencia, soportando aplicaciones como datos, audio, gráficas y aun video. Por ejemplo los dispositivos pueden incluir audífonos, teléfonos fijos, estereos o equipos de sonido, reproductores MP3.



Los consumidores de Bluetooth pueden:

- Hacer llamadas desde un headset conectado remotamente a un teléfono celular.
- Eliminar cables que enlazan computadores a impresores, teclados y el Mouse.
- Enganchar un reproductor MP3 inalámbricamente a otra maquina para descargar música.
- Configurar las redes del hogar de tal manera que se pueda monitorear remotamente el aire acondicionado, el horno, la navegación por Internet de los niños.
- Llamar a casa desde una ubicación remota para prender o apagar aparatos, colocar la alarma y actividades de monitoreo.

Como se apreció en las anteriores características, Bluetooth no usa ni depende de cables, a diferencia de otras redes que deben tener una o varias estaciones bases conectadas a la red principal mediante cables. La conexión sin cables se realiza gracias a un microchip

¹⁰ El nombre viene del rey Harald Blaatand (Diente Azul) de Dinamarca, quien vivió en el siglo X A.D. Diferente a sus contrapartes vikingas el rey Harald tenía el cabello oscuro (así, el nombre de Bluetooth, significa un aspecto oscuro). Fue famoso por llevar el cristianismo a lo largo de Escandinavia, uniendo Dinamarca y Noruega. El Logo azul que identifica los dispositivos dotados con Bluetooth es derivado de símbolos de sus iniciales.

CMOS de 9x9 que envía señales de radio de corto alcance y de alta frecuencia en la banda de 2.4 GHz. Los dispositivos deben traer este chip por defecto, si no lo traen no es posible adaptarlo posteriormente. Sin embargo, para los computadores personales, existen generalmente tarjetas tipo USB.

Bluetooth está diseñado para operar en un medio de muchos usuarios. Hasta ocho dispositivos se pueden comunicar en una pequeña red llamada *piconet*. Diez de estas piconet pueden coexistir en el mismo rango de cubrimiento del radio Bluetooth. Para ofrecer seguridad cada enlace es codificado contra traslapes e interferencias.

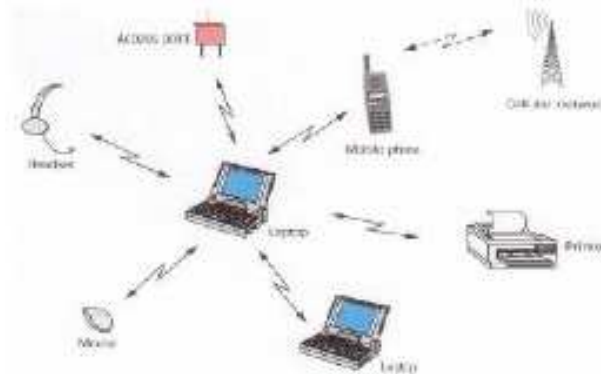


Figura A.1. Esquema general *piconet* Bluetooth

Fuente: www.bluetooth.com

A.1. USOS Y APLICACIONES BLUETOOTH.

Bluetooth provee soporte para tres áreas de aplicación general usando conectividad inalámbrica de rango-corto:

- **Puntos de acceso a voz y datos:** Bluetooth facilita la transmisión en tiempo real de voz y datos proporcionando conexión inalámbrica sin esfuerzo entre dispositivos de comunicaciones estacionarios y portátiles.
- **Reemplazo de cables:** Bluetooth elimina la necesidad para numerosos dispositivos de cables atados o adjuntos a los dispositivos de comunicaciones. Las conexiones son instantáneas y se mantienen aun cuando no existe línea de vista entre los dispositivos. El radio es de aproximadamente 10 m pero puede extenderse hasta 100 m con un amplificador opcional.
- **Red Ad-Hoc¹¹:** Un dispositivo equipado con un radio Bluetooth puede establecer conexión instantánea a otro radio Bluetooth tan pronto como este entra en su rango.

A continuación veremos algunos ejemplos o escenarios del uso de Bluetooth:

- Teléfono tres en uno.
Cuando se encuentra en la oficina el teléfono funciona como un intercomunicador (sin cargos de telefonía). En casa funciona como un teléfono sin cables (carga de

¹¹ Es una red creada de manera espontánea. No requiere una infraestructura formal y está limitada en espacio y extensión temporal. Se explicará más de redes ad-hoc en las secciones siguientes de redes WLAN.

línea fijo). Cuando se está en movimiento el teléfono funciona como un teléfono móvil (cargos de telefonía celular).

- **Puente Internet.**

Usando el computador portátil para navegar en Internet en cualquier lugar, si se está conectado inalámbricamente a través de un teléfono móvil (celular) o a través de una conexión cableada (PSTN, ISDN, LAN, xDSL).

- **Conferencia Interactiva.**

En reuniones y en conferencias, se puede compartir información instantáneamente con otros participantes. También se puede operar un proyector remotamente sin conexiones cableadas.

- **El último headset o manos libres.**

Conectando el headset al computador portátil o a cualquier conexión cableada y se liberan las manos para realizar funciones más importantes en la oficina o en el carro.

- **Maletín e-mail.**

Acceso al e-mail mientras el computador portátil esta aun en su maletín o estuche. Cuando el portátil reciba un mensaje e-mail, el teléfono móvil lo notificará. Se puede usar también el teléfono para buscar mensajes y correos electrónicos entrantes.

- **Mensajes retrasados.**

Se puede redactar un mensaje de correo electrónico mientras se esta en un avión. Cuando se aterriza y se puede cambiar al teléfono móvil, el mensaje será enviado inmediatamente.

- **Sincronización automática.**

Sincronización automática del computador de escritorio, computador portátil, agenda electrónica, y teléfono celular. Tan pronto cuando se ingrese a la oficina, la lista de direcciones y calendario en su agenda electrónica actualizara los archivos en su computador de escritorio o viceversa.

- **Tarjetas postales digitales instantáneas.**

Conectando una cámara de manera cableada al teléfono móvil o a cualquier otra conexión atada a cables, se adicionan comentarios desde el teléfono móvil, agenda digital o portátil, y se envían instantáneamente.

- **Computador de escritorio sin cables.**

Para conectar el computador de escritorio o computador portátil sin necesidad de cables a impresora, escaners, teclados, Mouse y a una red LAN.

- **Sector automovilístico.**

La mayoría de fabricantes se ha enfocado en la producción de manos libres para uso en el automóvil, otros productos que ofrecen las industrias incluyen lectores de CD, sistemas de navegación, altavoces, consolas de videojuegos.

A.2. ESTÁNDARES Y PROTOCOLOS.

Como se mencionó antes el estándar Bluetooth está definido en la norma 802.15 por la IEEE y son publicados por el consorcio Bluetooth SIG. Estos Estándares pertenecen a la familia 802 de la IEEE.

Los estándares Bluetooth presentan un grande y completo documento en volumen: más de 1500 páginas divididas en dos grupos: *Grupo Núcleo* y *Grupo Perfiles*.

El grupo de Especificaciones Núcleo describe los detalles de varias capas de la arquitectura Bluetooth, desde la interfase de radio hasta el control de enlace. Se cubren tópicos relacionados tales como interoperabilidad con tecnologías afines, requerimientos de prueba, y una definición de varios temporizadores Bluetooth y sus valores asociados.

Especificación de Versiones Núcleo:

- Versión 2.0 + Enhanced Data Rate (EDR), adoptada en Noviembre de 2004
- Versión 1.2, adoptada en Noviembre de 2003
- Versión 1.1, adoptada en Noviembre de 2001

Las Especificaciones Perfil, están relacionadas con el uso de tecnología Bluetooth para soportar varias aplicaciones. Cada especificación Perfil discute el uso de la tecnología definida en la especificación Núcleo para implementar un modelo de uso en particular. La especificación Perfil incluye una descripción de cuales aspectos de las especificación Núcleo son obligatorios, cuales opcionales y cuales no se aplican. El propósito de la especificación Perfil es definir un estándar de interoperabilidad, tal que productos de diferentes fabricantes y vendedores que ofrecen soporte a un modelo de uso dado trabajarán juntos.

En términos generales la Especificación Perfil cae en una de dos categorías: Reemplazo de cables o audio inalámbrico. El perfil de reemplazo de cables provee un significado conveniente para conexión lógica entre dispositivos y para intercambio de datos. Por ejemplo cuando dos dispositivos entran al rango del otro, automáticamente cada dispositivo le requiere al otro un perfil en común.

El perfil de audio inalámbrico tiene que ver con establecer conexiones de voz de rango corto.

Arquitectura de protocolos.

Bluetooth está definido como un protocolo de arquitectura en capas, consistente de protocolos de núcleo, protocolos de reemplazo de cables y control de telefonía, y protocolos adoptados.

➤ **Protocolos de núcleo.** Forman una capa de cinco elementos apilados que son:

Radio: Es un documento corto que especifica detalles de la interfaz de aire, incluyendo frecuencia, el uso de saltos de frecuencia, esquema de modulación y potencia transmitida. El rango de operación depende de la clase de dispositivos transmisores basados en la potencia de salida así:

- Dispositivos Clase 1: Potencia de salidas de 100 mW (+20dBm) para el máximo rango, con un mínimo de 1 mW (0dBm). En esta clase el control de la potencia es obligatorio, con rangos desde 4 a 20 dBm. Este modo provee las distancias más grandes con rangos de 100 m o 300 pies.

- Dispositivos Clase 2: Potencia de salida máxima de 2.4 mW (+4dBm) con un mínimo de 0.25 mW (-6dBm). El control de potencia es opcional. Tienen un rango de 10 m o 30 pies.
- Dispositivos Clase 3: Potencia de salida nominal de 1 mW La potencia mas baja, tienen un rango de hasta 1 m o 3 pies.

Bluetooth hace uso de la banda de 2.4 – 2.485 GHz, que esta dentro de la banda ISM (Industrial, Scientific and Medical). En la mayoría de los países, la banda es suficiente para definir 79 canales de 1 MHz. La modulación usada es modulación Gaussiana FSK, '1' binario que representa una desviación de una frecuencia positiva y un '0' binario que representa una desviación de una frecuencia negativa, de una frecuencia central. La desviación mínima es de 115 kHz.

Banda base: Respectivo al establecimiento de conexión dentro de una *piconet*, direccionamiento, formato de paquetes, tiempo, y control de potencia. Es uno de los más complejos documentos de las especificaciones Bluetooth. Trata elementos claves como los saltos de frecuencia Frequency Hopping (FH), enlace físico, canales lógicos, corrección de errores, canales de control, seguridad, audio Bluetooth.

La tasa de salto de frecuencia es de 1600 saltos por segundo, así cada canal físico es ocupado durante 0.625 ms. Cada periodo de tiempo de 0.625 ms se refiere a un spot, y estos slots están numerados secuencialmente.

La tasa de datos es de 1 Mbps para la Versión 1.2, y de hasta 3 Mbps para la Versión 2.0 + EDR.

El FH en Bluetooth fue diseñado para reducir la interferencia entre tecnologías inalámbricas que comparten la banda de 2.4 GHz. Las especificaciones de Radio y Banda base se resumen en la siguiente tabla:

Topología	Hasta 7 enlaces lógicos en estrella
Modulación	GFSK
Tasa pico de datos	1 Mbps
Ancho de Banda RF	220 kHz (-3dB), 1 MHz (-20dB)
Banda RF	2.4 GHz, banda ISM
Portadores RF	23 / 79
Espaciamiento Portadoras	1 MHz
Potencia de Transmisión	0.1 W
Acceso Piconet	FH – TDD – TDMA
Tasa salto de frecuencia FH	1600 saltos/s
Acceso Scatternet	FH - CDMA

Tabla A.1. Parámetros de Radio y Banda Base Bluetooth

Link Manager Protocol (LMP). Protocolo Administrador de Enlace. Es el responsable de la configuración del enlace entre dispositivos Bluetooth y la administración del enlace saliente. Esto incluye aspectos de seguridad como autenticación y encriptación, más el control y la negociación del tamaño de los paquetes banda base.

Logical Link Control and Adaptation Protocol (L2CAP). Protocolo de Control de Enlace Lógico y de Adaptación. Adapta los protocolos de capas superiores a la capa bandabase. L2CAP provee ambos tipos de conexiones, orientadas a conexión y no orientadas a conexión.

Service Discovery Protocol (SDP). Protocolo Descubridor de Servicios. Información del dispositivo, servicios y características de los servicios que pueden ser requeridos para establecer la conexión entre dos o más dispositivos Bluetooth.

➤ **Protocolos de Reemplazo de Cables.** RFCOMM es el protocolo de reemplazo de cables incluido en la especificación Bluetooth. RFCOMM presenta un puerto serial virtual que está diseñado para hacer el reemplazo de tecnologías tan transparente como sea posible. Los puertos seriales tienen una de las más comunes interfaces de comunicación usadas con computadores y dispositivos de comunicación. Por lo tanto, RFCOMM permite el reemplazo de cables de puerto serial con el mínimo de modificaciones de dispositivos existentes. RFCOMM se provee para transporte binario de datos y emula señales de control EIA-232 sobre la capa banda base Bluetooth.

EIA-232 (antiguamente conocido como RS - 232) es la interfase estándar de puerto serial más ampliamente usada.

➤ **Protocolo de Control de Telefonía.** Bluetooth especifica un protocolo de control de telefonía, TCS BIN, Telephony Control Specification-Binary es un protocolo orientado a bits que define la llamada de señalización de control para el establecimiento del diálogo y llamadas de datos entre dispositivos Bluetooth. Adicionalmente, define los procedimientos de administración de la movilidad para el manejo de grupos de dispositivos Bluetooth TCS.

➤ **Protocolos Adoptados.** Están definidos en especificaciones emitidas por otras organizaciones que hacen estándares e incorporada en la arquitectura completa Bluetooth. La estrategia Bluetooth es para inventar solo los protocolos necesarios y usa los estándares existentes donde sea posible. Los protocolos adoptados incluyen los siguientes:

- PPP: Point-to-Point Protocol, Protocolo Punto a Punto es un protocolo estándar de Internet para transportar datagramas IP sobre un enlace punto a punto.
- TCP/UDP/IP: Estos son los protocolos base del protocolo TCP/IP.
- OBEX: Object Exchange Protocol. Protocolo de intercambio de objetos, es un protocolo de nivel-sesión desarrollado por IrDA (Infrared Data Association) para el intercambio de objetos. OBEX provee funcionalidad parecida al http, pero de manera más simple. También provee un modelo de representación de objetos y operaciones. Ejemplos de estos objetos transferidos por OBEX son los calendarios virtuales vCalendar y tarjetas virtuales vCards.
- WAE/WAP: Bluetooth incorpora el Wireless Application Environment, medio de aplicaciones inalámbricas y el Wireless Application Protocol dentro de esta arquitectura.

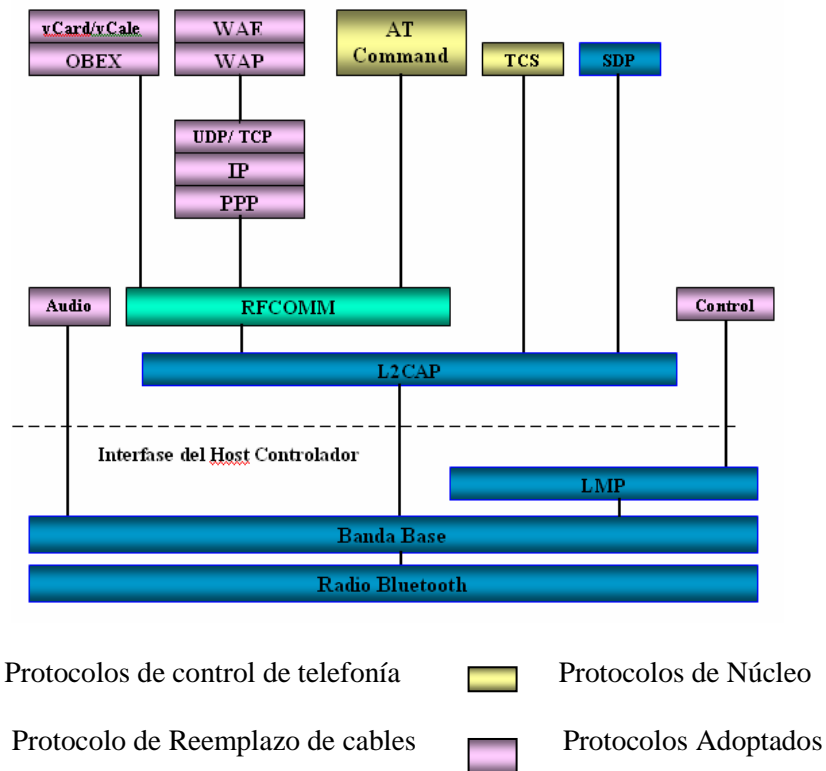


Figura A.2. Pila de Protocolos Bluetooth

A.3. SEGURIDAD

La seguridad Bluetooth está definida en las especificaciones Banda Base y consiste de los siguientes elementos:

- Autenticación
- Encriptación (Privacidad)
- Administración y Uso de Clave

Los algoritmos de seguridad hacen uso de cuatro parámetros:

- **Dirección Unidad:** Dirección del dispositivo de 48 bits, el cual es públicamente conocido.
- **Clave de Autenticación Secreta:** Una clave secreta de 128 bits.
- **Clave Secreta de Privacidad:** Una clave secreta de longitud de 4 a 128 bits.
- **Numero Randómico:** Un número randómico de 128 bits derivado de un algoritmo de generación pseudorandómico ejecutado en la unidad Bluetooth.

Las dos claves son generadas y configuradas con la unidad y no son reveladas.

El propósito de la autenticación es verificar la identidad de uno de los dos dispositivos Bluetooth envueltos en un intercambio. La autenticación es ejecutada para verificar que dos dispositivos comparten la misma clave de autenticación preconfigurada. Para comenzar este proceso un dispositivo A genera un número aleatorio $AU_RAND_A^{12}$ y transmite este valor al dispositivo B.

En la **Figura A.3. (a)** y **A.3. (b)** se ilustra esta autenticación.

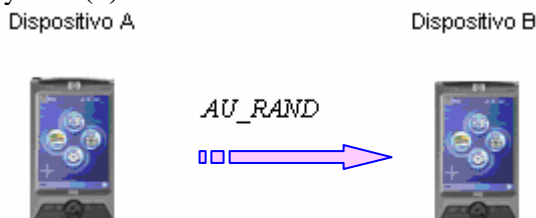


Figura A.3. (a) Proceso Autenticación Bluetooth. Inicio de diálogo

Ambos lados utilizan el algoritmo de autenticación E_1 para generar una señal de respuesta de 32 bits $SRES$. El algoritmo E_1 toma como valor de entrada AU_RAND_A , la dirección $BD_ADDR_B^{13}$ de 48 bits del dispositivo B y la clave secreta compartida y genera una salida de 128 bits; 32 bits de esta salida forman $SRES$. El algoritmo E_1 está basado en el algoritmo de encriptación SAFER y genera un MAC (Message Authentication Code), el cual es un código ‘molido’ de la entrada basado en la clave secreta. Después que B ha generado este $SRES$, retorna este valor a A. El dispositivo A compara el valor entrante de $SRES$ con el valor que ha generado. Si los dos valores concuerdan B es autenticado.



Figura A.3. (b) Proceso Autenticación Bluetooth. Respuesta y comparación

Las dos figuras anteriores muestran el proceso de autenticación solo en un sentido. La autenticación mutua se lleva a cabo con el mismo intercambio cuando el dispositivo B inicia el diálogo.

La información del usuario puede ser protegida mediante la encriptación del paquete. El código de acceso y el encabezado del paquete nunca son encriptados. El proceso de

¹² AU_RAND : Authentication Random Number

¹³ BD_ADDR : Bluetooth Device Address

encriptación se lleva a cabo usando un algoritmo de encriptación conocido como algoritmo E_0 . En una configuración maestro-esclavo cuando la encriptación es habilitada, el dispositivo maestro envía un número randómico RAND al dispositivo esclavo. Por cada paquete de transmisión, una nueva clave de encriptación es generada así:

Primero, una clave de paquete es generada combinando una forma compleja RAND, la dirección del dispositivo maestro, el valor actual de reloj, y una clave secreta compartida. Esta clave de paquete es usada como entrada a E_0 para producir un flujo continuo de bits. El algoritmo E_0 es de la forma de un cambio de registro de realimentación lineal LFSR (Linear Feedback Shift Register) que usa la clave del paquete para la inicialización de LSFR. Debido a que el valor de reloj cambia para cada encriptación, una clave de paquete diferente es usada cada tiempo, mejorando la seguridad.

ANEXO B. TECNOLOGIA WAP

Wireless Application Protocol. Protocolo de Aplicación Inalámbrica. Aparece en el ámbito de los dispositivos móviles de bolsillo como PDAs y teléfonos celulares. Fue acordado por los principales fabricantes de teléfonos celulares, Motorola, Nokia, Sony-Ericsson, en 1997, posteriormente se unieron otros fabricantes y empresas formando el WAP Forum, grupo para la estandarización.

WAP está diseñado para trabajar con todas las tecnologías de red wireless, por ejemplo GSM, CDMA y TDMA.

Los fuertes efectos presentes en el uso de los dispositivos y especialmente teléfonos móviles y terminales para servicios de datos, están reflejados en las limitaciones que estos tienen en cuanto a procesador, capacidad de memoria y tiempo de vida de la batería. También la interfaz de usuarios es limitada y los displays o pantallas son pequeños.

Las redes inalámbricas se caracterizan por tener bajo ancho de banda, latencia alta y disponibilidad impredecible comparadas con las redes cableadas. Además todas estas características varían ampliamente de dispositivo a dispositivo y de red a red. Finalmente los usuarios móviles tienen diferentes necesidades y expectativas de otros usuarios de sistemas de información. Por ejemplo, los terminales móviles deben ser mucho más fáciles de usar que las estaciones de trabajos y computadores personales.

La tecnología WAP está diseñada para tratar con todos estos cambios y retos.

B.1. USOS Y APLICACIONES WAP

El estándar WAP une dos entornos que están creciendo de manera acelerada como son el Internet y la comunicación inalámbrica. Esta característica le permite:

- Independencia. Independencia en la clase de dispositivo que usa: celular, computador personal, PDAs, etc. Independencia en la utilización de estándares para realizar aplicaciones de redes de telefonía. WAP es escalable y abierto. Independencia en el sistema de transporte usado: TDMA, GSM, etc.
- Adaptabilidad a nuevas tecnologías de transporte como GPRS, UMTS.
- Accesibilidad. Fácil y seguro acceso a servicios tan importantes de Internet como mensajería, entretenimiento y banca a distancia. Acceso a cualquier otro contenido de la Red, con solo llevar un dispositivo compatible con esta tecnología.
- En el sector empresarial el envío de correos electrónicos y faxes al servidor de la intranet para el posterior reenvío o difusión de correos electrónicos a los teléfonos móviles de la compañía a menor costo.
- Acceso a las bases de datos de la compañía, así como información de trabajos en grupo, programación de viajes, agendas, reuniones o juntas, etc.
- En el sector o nivel de usuarios particular, el acceso a las últimas y actuales noticias desde el teléfono móvil, carteleras de cine con información actualizada

periódicamente como horarios, taquillas, salas, anuncios clasificados, información meteorológica como estado del clima, preedición de viajes a 24 o 48 horas, imágenes vía satélite, guía turísticas con información de hoteles, sitios de interés, eventos, etc.

Las aplicaciones y servicios WAP se han dividido en dos tipos: por un lado las aplicaciones generales que se pueden hacer para un Servidor Web normal que permita WML y WMLS. Por otro las aplicaciones específicas que pueden usar el Servidor WTA. Respecto a esta clase de servidores y aplicaciones WML, WMLS y WTA se hablará en la sección siguiente. A continuación veremos algunos escenarios del uso de la tecnología WAP, dependiendo el servicio y el servidor requerido.

Aplicaciones generales al Servidor Web que acepte WML, WMLS.

En general las aplicaciones y servicios, son del mismo tipo que las aplicaciones Web, aplicaciones muy conocidas y cotidianas y que seguramente alguna vez las hemos utilizado.

- Consulta de todo tipo de información y noticias:
 - Últimas noticias de política, sociedad, economía, cultura.
 - Noticias y novedades del mundo del deporte
 - Programación diaria de las cadenas de televisión
 - Cartelera de los cines
- Consulta de documentos remotos.
 - Servicios de banca y comercio electrónico.
 - Acceso a aplicaciones corporativas residentes en redes locales o intranets.
 - Servicio de E-mail, novedades o News y otros servicios que ofrecen los operadores de telefonía.

Acceso a todo tipo aplicaciones corporativas residentes en redes locales o intranets, como por ejemplo:

- Envío de faxes y correos electrónicos al servidor de la Intranet
- Envío de correos electrónicos a los móviles de la compañía
- Agenda
- Acceso a la base de datos de la compañía

Aplicaciones al servidor WTA

El servidor WTA Wireless Telephony Application, da acceso WAP a las facilidades proporcionadas por la infraestructura de telecomunicaciones del proveedor de acceso a la red. Las posibles aplicaciones que se pueden ofrecer con este servidor son las siguientes:

Acceso a los datos de una Intranet local, por medio de la cual, los abonados podrían consultar:

- Factura de teléfono.
- Servicios ofrecidos.
- Buzones de sugerencias.

- Mensajes cortos entre móviles.

Sin embargo WAP presenta algunas incompatibilidades e inconvenientes debido al gran número de fabricantes y modelos de teléfonos celulares.

- Incompatibilidades entre los diferentes dispositivos terminales y el lenguaje WML¹⁴, de modo que las diferentes aplicaciones no funcionan de igual manera en todos los teléfonos.
- El micronavegador de los dispositivos solo puede leer información escrita en lenguaje WML, así, para acceder a la información los operadores y las compañías de telefonía móvil tienen que desarrollar contenidos propios o adoptar contenidos ya existentes.
- La velocidad limitada en acceso a Internet esta en contra de la proliferación de esta tecnología.
- Los altos precios de este servicio ofrecidos por los operadores.
- Los contenidos y páginas Web no se ven de igual forma que un computador ordinario. Los formatos de fotografía en las páginas WAP solo pueden tener formatos en blanco y negro y de baja calidad.

B.2. ESTÁNDARES Y PROTOCOLOS.

El WAP Forum lanzó en Junio de 2000 la versión v1.2 de WAP. Existen actualmente múltiples versiones de WAP, pero las que fueron comercializadas fueron WAP 1.1, WAP 1.2 y WAP 2.0.

WAP combina protocolos para la comunicación inalámbrica entre un usuario móvil e Internet, como acceso a correo electrónico y Web. Está basado en los actuales estándares de Internet, tales como IP, XML, HTML y HTTP.

El modelo de Programación de WAP esta basado en tres elementos:

- El cliente.
- La puerta de enlace o gateway.
- El servidor original.

HTTP es usado entre la puerta de enlace y el servidor original para transferir el contenido. La puerta de enlace actúa como un servidor Proxy para el dominio wireless. Por ejemplo, la puerta de enlace o gateway provee servicios DNS, convierte entre protocolos WAP y protocolos Web como HTTP, , codifica información de la Web en información mas compacta que minimiza la comunicación inalámbrica, y, en la dirección de decodificación, lo hace a estas formas compactas en convencionales comunicaciones de estándar Web.

En un medio WAP un usuario móvil puede buscar contenido Web en un servidor Web ordinario. El servidor Web provee contenido en forma de páginas en código HTML que son transmitidas usando la pila de protocolos estándar Web tales como HTTP/TCP/IP. El contenido HTML debe pasar a través de un filtro HTML, el cual puede también estar ubicado con el servidor proxy o en un módulo físico separado. Este filtro traslada el

¹⁴ Wireless Markup Language. Se mencionará en la siguiente sección Estándares y Protocolos.

contenido HTML en contenido WML. Si el filtro esta separado del proxy, HTTP/TCP/IP es usado para entregar el WML al proxy.

El proxy convierte el WML a una forma mas compacta conocida como WML binario y lo entrega al usuario móvil sobre una red inalámbrica usando la pila de protocolos WAP.

Si el buscador Web es capaz de generar directamente el contenido WML, entonces es entregado usando HTTP/TCP/IP al proxy, el cual convierte el WML a WML binario y entonces lo entrega al nodo móvil usando protocolos WAP. En la siguiente figura se muestran los componentes claves de un medio WAP:

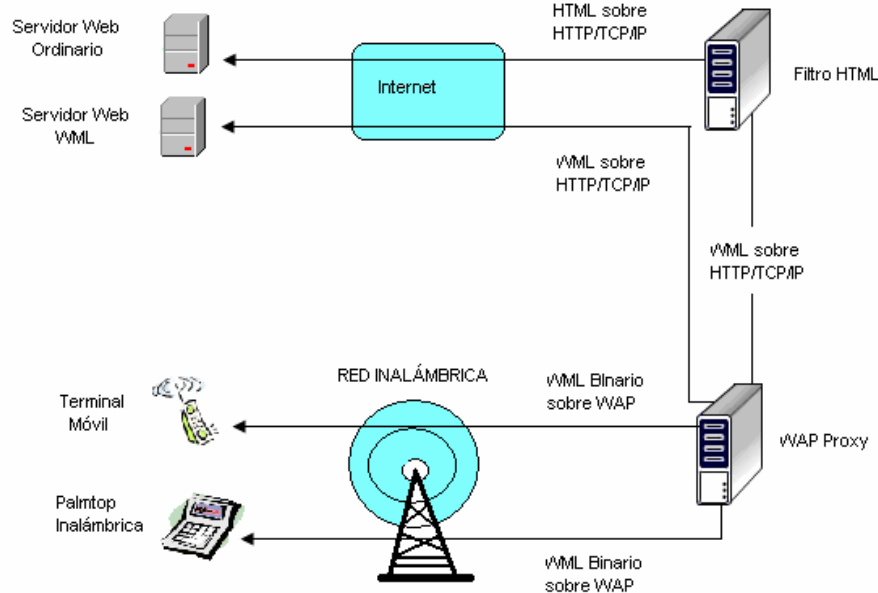


Figura B.1. Infraestructura WAP

Para ilustrar más el funcionamiento de una red WAP, se mostrará el siguiente ejemplo, donde el cliente WAP se comunica con dos servidores a través de la red, con el proxy WAP y con el servidor WTA y veremos las labores y pasos de estos dos servidores. La ilustración de esta red se muestra en la **Figura B.2.** Ejemplo de una red WAP.

El Proxy WAP: Se encarga de dos labores:

- Traducir la petición WAP, escrita en WML, a una petición WWW, permitiendo así que el cliente WAP pueda realizar peticiones al servidor Web.
- Codificar las respuestas del servidor a un formato binario de modo que sea entendible por el cliente WAP.

El Servidor WTA, Wireless Telephony Application, puede responder las peticiones WAP del cliente directamente; de este modo, permite ofrecer acceso WAP a determinadas características de la infraestructura de comunicaciones del operador de red.

El Servidor Web. Se comunica con el Proxy WAP de dos posibles modos:

- Si el servidor Web proporciona un contenido WAP, como por ejemplo WML o WMLS, entonces no se necesita ningún filtro HTML.
- Si el servidor Web proporciona un servicio WWW, como HTML, entonces se usa un filtro HTML para traducir el contenido WWW en uno WAP. Como se ve en el

ejemplo, el filtro HTML, puede encargarse de traducir una respuesta HTML en una WML, y devolvérsela al Proxy WAP.

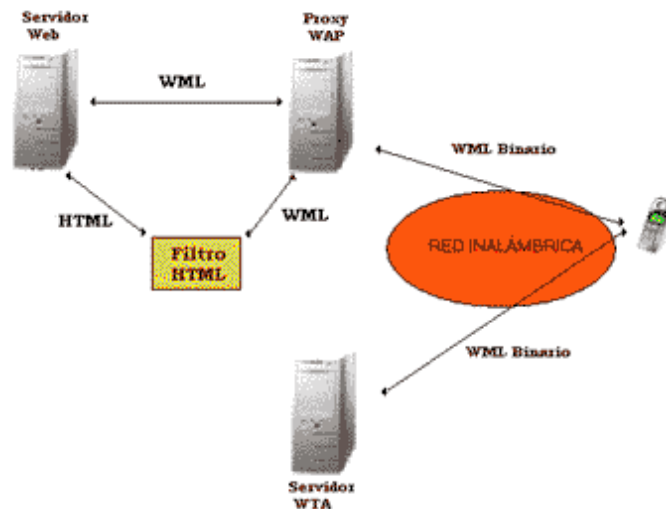


Figura B.2. Ejemplo de una red WAP

Fuente: www.programatium.com

WAParea – Manual WAP Virginia Miñaur Aznar

Arquitectura de Protocolos.

La especificación WAP incluye lo siguiente:

- Un modelo de programación basado en el Modelo de Programación WWW.
- Un lenguaje de marcado, el Lenguaje de Marcado Wireless WML, adhiriéndose al XML.
- Una especificación para un buscador ubicado en un móvil, terminal inalámbrico.
- Una pila de protocolos de comunicación liviana.
- Un marco para aplicaciones de telefonía inalámbrica WTAs (Wireless, Telephony Applications), para poder integrar las aplicaciones de telefonía al teléfono celular.

Esta especificación consiste de un número de protocolos y de módulos (llamada pila de protocolos WAP) que tienen una relación con otros protocolos como por ejemplo GSM, UDP, IP. Estos protocolos son WML, WMLScript, WAE, WSP, WTP, WTLS, WDP.

WML (Wireless Markup Language). El Lenguaje de Marcado Inalámbrico fue diseñado para describir contenido y formatos presentando datos en dispositivos con limitado ancho de banda, limitado tamaño de pantalla, y limitada capacidad de entrada. WML permite el escalamiento de displays sencillos en displays de dos líneas en dispositivos pequeños, así como pantallas más grandes en teléfonos inteligentes. Para un computador ordinario, un buscador Web proporciona contenido en forma de páginas Web codificadas con HTML. Para traducir una página Web codificada en HTML en WML con contenido y formato ubicable en un dispositivo inalámbrico, mucha de la información especialmente gráficas y animaciones debe ser eliminada. WML presenta principalmente

información basada en texto que apunta a la captura de la información esencial de una página Web.

WMLScript. Es un lenguaje de escritura con similitudes a JavaScript. Está diseñado para definir programas tipo escritura en un dispositivo usuario con limitada capacidad de procesamiento y de memoria. Las capacidades más importantes de WMLScript incluyen lo siguiente:

- Revisar la validez de la entrada de un usuario antes de ser enviado al servidor de contenidos.
- Facilidades de acceso a los dispositivos y a los periféricos.
- Interactuar con los usuarios sin introducir recorridos de ida y vuelta al servidor origen, por ejemplo mostrar un mensaje de error.

WAE (Wireless Application Environment). Especifica un marco de aplicación para dispositivos inalámbricos tales como teléfonos móviles, PDAs, beepers, y pagers. Consiste de herramientas y formatos que han sido desarrollados para facilitar las tareas de desarrollo de aplicaciones y dispositivos soportados por WAP.

Es un entorno de aplicación de propósito general, basado en la combinación del World Wide Web y tecnologías de Comunicaciones Móviles.

Este entorno incluye un micro navegador, que posee las siguientes funcionalidades:

- El lenguaje WML del cual ya hablamos arriba.
- El lenguaje WMLScript del cual igualmente ya mencionamos.
- WTA (Wireless Telephony Applications), es un entorno para aplicaciones o servicios de telefonía.
- WTAI (Wireless Telephony Application Interface), es una interfaz utilizada en los terminales móviles para operaciones locales de control de llamadas (recepción, iniciación y terminación) y acceso a listados telefónicos.

WSP (Wireless Session Protocol). Proporciona aplicaciones con una interfase para dos servicios de sesiones. En esencia WSP está basado en HTTP con algunas adiciones y modificaciones para optimizar el uso sobre canales inalámbricos.

Este protocolo proporciona a la Capa de Aplicación (WAE) interfaz con dos servicios de sesión:

- Un servicio orientado a conexión que funciona por encima de la Capa de Transacciones (WTP).

- Un servicio no orientado a conexión que funciona por encima de la Capa de Transporte WTP, y que proporciona servicio de datagramas seguro o no seguro.

Esta capa proporciona las siguientes funcionalidades:

- Establecimiento y liberación de conexiones entre cliente y servidor.,
- Intercambio de información entre cliente y servidor.
- Negociación de las características del protocolo.
- Suspensión y reanudación de la sesión.

WTP (Wireless Transaction Protocol). Maneja transacciones convirtiendo peticiones y respuestas entre un usuario agente (como un buscador WAP) y un servidor de aplicación para tales actividades, como buscadores y transacciones de comercio electrónico.

Este protocolo funciona por encima de un servicio de datagramas ya sean seguros como no seguros, y proporciona las siguientes funcionalidades:

- Proporciona los servicios necesarios para soportar las transacciones, estos servicios pueden ser de tres clases:
 - Peticiones inseguras de un solo camino
 - Peticiones seguras de un solo camino
 - Transacciones seguras de dos caminos
- También proporciona seguridad en las transacciones.

WTLS (Wireless Transport Layer Security). La Capa Inalámbrica de Seguridad de Transporte WTLS es el protocolo basado en el estándar TLS, Transport Layer Security (Seguridad en la Capa de Transporte), el cual es un refinamiento del estándar SSL, Secure Sockets Layer. TLS es el protocolo estándar de seguridad utilizado entre los buscadores Web y los servidores Web. WTLS es más eficiente que TLS pues requiere intercambio de mensajes más pequeños. Es entonces utilizado en el entorno Web, para la seguridad en la transferencia de datos. WTLS provee seguridad entre el dispositivo móvil cliente y el gateway WAP, para proveer seguridad fin-a-fin; TLS es usado en cambio entre el gateway y el servidor objetivo.

Las funcionalidades de esta capa son las siguientes:

Integridad de los datos, Privacidad de los datos, Autenticación y Protección de servicio denegado.

WDP (Wireless Datagram Protocol). WDP es utilizado para adatar una capa mas alta de protocolo WAP al mecanismo de comunicación (llamado el portador) móvil y el *gateway* WAP. Esta adaptación puede incluir la partición de los datos en segmentos de tamaño apropiado para el portador y para la interfase con red del portador.

El Protocolo Inalámbrico de Datagramas WDP proporciona las siguientes funcionalidades:

- Proporciona un servicio fiable a los protocolos de las capas superiores de WAP.
- Permite la comunicación de forma transparente sobre los protocolos portadores: CDMA, SMS, GSM...

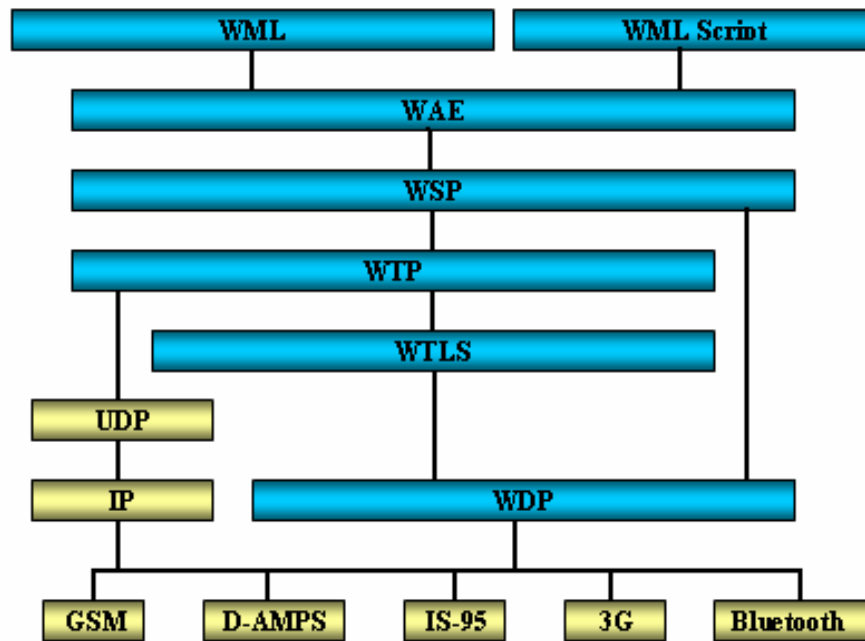


Figura B.3. Pila de Protocolos WAP

B.3. SEGURIDAD.

La seguridad en WAP esta encargada por la capa WTLS, que constituye una capa modular, que depende de la seguridad requerida para el tipo de aplicación determinada. Esta capa proporciona a las capas de nivel superior de WAP una interfaz de servicio de transporte seguro que preserva la interfaz de transporte subyacente, además proporciona una interfaz de gestión de conexiones seguras.

El objetivo de esta capa es brindar:

- Privacidad. Asegura que los datos entregados entre un terminal y un servidor de aplicaciones no pueden ser entendidos por terceros que puedan interceptar el flujo de información.
- Integridad de datos. Asegura que los datos intercambiados entre el terminal y el servidor de aplicaciones no ha sido modificada ni que la información esta corrupta.
- Autenticación entre dos aplicaciones de aplicaciones. Este protocolo contiene servicios para establecer la autenticidad del dispositivo terminal y del servidor de aplicaciones.
- Protección de servicio denegado: De manera adicional WTLS proporciona una interfaz para el manejo de conexiones seguras como el caso de operaciones comerciales electrónicas entre dispositivos móviles, detectando y rechazando mensajes que han sido reenviados o no han sido satisfactoriamente verificados.

Con las siguientes características:

- Soporte de Datagramas.
- Mecanismos de negociación optimizados.
- Refresco dinámico de claves.

Se sitúa como la capa opcional sobre la capa de transporte. Este protocolo ha sido diseñado especialmente para los protocolos de transporte WAP y optimizado para ser usado en los canales de comunicación de banda estrecha.

El protocolo WTLS toma los mensajes que hay que transmitir, comprime opcionalmente, aplica mecanismos MAC, cifra los datos y transmite el resultado. Los datos recibidos son descifrados, verificados y descomprimidos y luego son entregados a los clientes de nivel superior.

El modelo de seguridad WAP puede dividirse en dos partes separadas por la pasarela WAP, primero ésta usa el estándar SSL, para establecer una comunicación segura con el servidor Web, asegurando la integridad, privacidad y autenticidad del servidor.

Por otro lado la pasarela recoge los mensajes codificados con SSL del servidor Web y los transforma para transmitirlos usando WAP y la capa de seguridad WTLS. Las peticiones desde el teléfono hacia el servidor recorren el camino inverso, de esta manera la pasarela se encarga de hacer la conversión recíproca entre los protocolos WTLS y SSL.

La necesidad del cambio de SSL a WTLS viene impuesta por la naturaleza de las comunicaciones inalámbricas: ancho de banda reducido con alta latencia; debido a que SSL se diseñó para ser usado por computadores de escritorio con capacidades de procesamiento superiores a las de un teléfono celular y con mayor ancho de banda y menor latencia.

La transformación entre SSL y WTLS tiene una duración de milisegundos y ocurre en la memoria de la pasarela de manera simultánea a otras miles de peticiones de otras pasarelas de otros usuarios. Para permitir una conexión virtual y segura entre los protocolos, se debe tener protegida a la pasarela con las siguientes medidas:

- La pasarela nunca guarda el contenido decodificado en algún tipo de medio secundario.
- El proceso de decodificación / codificación está desarrollado bajo unos parámetros de seguridad optimizados en velocidad, tal que el contenido original sea borrado de la memoria volátil de la pasarela tan pronto como sea posible.
- Restringiendo el acceso físico a la consola de la pasarela.
- Restringiendo el acceso físico administrativo a la pasarela, a las direcciones internas del firewall del operador.

Las aplicaciones WAP permiten habilitar o deshabilitar las propiedades del protocolo WTLS dependiendo de los requerimientos y de las especificaciones de la red en particular, por ejemplo la privacidad puede ser deshabilitada en una red que ya posea esta característica en una capa inferior.

ANEXO C. TECNOLOGÍA WLAN

Las WLANs están generalmente categorizadas de acuerdo a la técnica de transmisión que es usada. Todos los actuales productos de WLANs caen en una de las siguientes categorías:

LANs Infrarrojo (IR LANs). Una celda individual de una IR LAN está limitada a un simple cuarto porque la luz infrarroja no penetra paredes opacas.

Las comunicaciones ópticas inalámbricas en la porción del infrarrojo del espectro son comunes en la mayoría de los hogares, donde es usada por una variedad de dispositivos de control remoto. Recientemente la atención ha girado al uso de esta tecnología en el diseño de WLANs. Hay tres alternativas de técnicas de transmisión comúnmente usadas para transmisión de datos IR: La señal transmitida puede ser concentrada y apuntada (como en un control remoto para TV); puede ser radiada omnidireccionalmente; o puede ser reflejada de un techo pintado sin colores opacos.

LANs de Espectro Esparcido (*Spread Spectrum*). Este tipo de LANs hace uso de la tecnología de transmisión del espectro esparcido. En la mayoría de los casos estas LANs operan en la bandas ISM (Industrial, Scientific, and Medical) tanto que la licencia FCC no es requerida para su uso en USA.

Actualmente este es el tipo más popular de WLANs y el interés se centrará en hablar y tratar las redes de este tipo.

Microondas Banda estrecha. Estas LANs operan a frecuencias microondas pero no usan el espectro esparcido. Algunos de estos productos operan a frecuencias que requieren licencia FCC, mientras que otras usan una de las bandas ISM sin licencia.

WLAN es un sistema de comunicaciones de datos flexible, implementado como una extensión o alternativa a las redes cableadas de área local LAN (*Local Area Network*) instaladas en edificios o campos universitarios. Corresponden a una variación de la red local tradicional LAN que utiliza ondas de radio de alta frecuencia, en lugar del par trenzado, cable coaxial o la fibra óptica, cumpliendo las funciones de comunicaciones propias de una red tradicional como transferencia de archivos, periféricos compartidos, correo electrónico y acceso a bases de datos.

No se espera que las redes inalámbricas reemplacen a las redes cableadas, pues estas alcanzan y superan las velocidades de transmisión de las redes inalámbricas. Mientras que con la tecnología inalámbrica se alcanza velocidades de hasta 54 Mbps con la tecnologías cableadas Ethernet y Fast Ethernet se alcanza velocidades hasta de 100 Mbps, también se logran velocidades de 1000 Mbps con Gigabit Ethernet y se espera alcanzar 10000 Mbps. Con los sistemas de fibra óptica se alcanzan velocidades mayores. Actualmente se están fabricando y comercializando dispositivos inalámbricos con velocidades de 108 Mbps, pero su difusión ha sido muy lenta.

En la siguiente tabla, **Tabla C.1.** se muestran las principales características de las tecnologías LAN mencionadas:

	LAN Infrarrojo		LAN Espectro Esparcido		Microonda
	Difuso	Haz Dirigido	FHSS	SDSS	Banda Estrecha
Tasa Trans. Mbps	1 a 4	1 a 10	1 a 3	2 a 20	10 a 20
Rango en m	15 a 60	25	30 a 100	30 a 250	10 a 40
Detectabilidad	Negada	Negada	Poca	Poca	Alguna
Long.Onda nm/Frecuencia	L: 800 a 900	L: 800 a 900	902 a 928 MHz 2.4 a 2.4835 GHz 5.725 a 5.85 GHz	902 a 928 MHz 2.4 a 2.4835 GHz 5.725 a 5.85 GHz	902 a 928 MHz 5.2 a 5.775 GHz 18.825 a 19.205 GHz
Técnica modulación	ASK	ASK	FSK	QPSK	FS / QPSK
Potencia radiada	—	—	< 1 W	< 1 W	25 mW
Licencia	No	No	No	No	Si, menos ISM
Método Acceso	CSMA	Token Ring, CSMA	CSMA	CSMA	ALOHA, CSMA

Tabla C.1. Comparación de Tecnologías Inalámbricas según categorías

La WLAN se compone fundamentalmente de dos elementos:

- Puntos de acceso AP (Access Point).
- Dispositivos clientes o estaciones STA.

Algunos autores especifican de la siguiente manera:

- APs
- STAs
- Tarjetas NIC, Network Interface Card, para acceso inalámbrico.

Los puntos de acceso APs actúan como *hubs* o concentradores que envían y reciben información vía ondas de radiofrecuencia (RF) hacia y desde un PC u otro tipo de dispositivo más ligero y móvil, como un Notebook y un PDA o Palmtop, equipados con tarjetas de red inalámbricas, Wireless NIC. El punto de acceso puede ser un aparato en sí que forma parte de la base de la red o la conecta por medio de cables a una LAN convencional. Los usuarios pueden enlazar múltiples puntos de acceso a una LAN, creando segmentos inalámbricos en todas sus instalaciones.

Las tarjetas de acceso inalámbrico, Wireless NIC se usan para comunicarse con el punto de acceso AP, cada STA, computadora portátil o de escritorio necesita una tarjeta especial para redes inalámbricas. Al igual que las tarjetas de interfaz para redes (NICs) de las redes tradicionales, estas tarjetas permiten que los aparatos se comuniquen con el punto de acceso. Se instalan fácilmente en las ranuras PC de las computadoras portátiles, a las ranuras PCI de los dispositivos de escritorio, o se enlazan a puertos USB. Además, un usuario puede conectar cualquier otro dispositivo que no tenga una ranura para Tarjetas PC o PCI a su red inalámbrica, al usar un Ethernet Client Bridge, ECB que funciona con cualquier dispositivo que cuente con puerto Ethernet, puerto serial o puerto USB como impresoras o escáneres. Una vez que se conecta el punto de acceso a una toma de poder y los aparatos en red están debidamente equipados con tarjetas inalámbricas, las conexiones de red se hacen automáticamente cuando estos aparatos se encuentren dentro del campo de alcance del hub. El campo de alcance de una red inalámbrica en ambientes estándares de oficinas puede ser de varios cientos de metros.

C.1. USOS Y APLICACIONES WLAN

Básicamente existen cuatro áreas de aplicación para las WLANs:

- Ampliación de redes LAN
- Interconexión de edificios
- Acceso nómada
- Redes ad hoc.

- **Ampliación de redes LAN**

Una LAN inalámbrica ahorra los costos de instalación de redes cableadas y facilita la tarea de reubicación y otras modificaciones a la estructura de la red. Estas motivaciones para LANs inalámbricas no ha sido suficientes para su completa expansión, los arquitectos han construido los nuevos edificios pensados en la implementación y extensión de aplicaciones de datos cableadas. Aunado a esto el desarrollo y los avances en la tecnología de transmisión de datos hay una creciente demanda de cable par trenzado blindado y no blindado, STP y UTP, en especial UTP Categoría 3 y Categoría 5.

Sin embargo, en un gran número de ambientes, existe un papel para las redes inalámbricas como alternativa de redes cableadas. Por ejemplo en grandes edificios con grandes áreas y extensiones que pueden incluir campos deportivos o grandes parqueaderos, tales como plantas industriales, grandes depósitos, almacenes con despensas y vitrinas, edificios históricos con insuficiente par trenzado y edificios donde está prohibido abrir nuevos agujeros y/o taladrar y pequeñas oficinas donde el mantenimiento e instalación de LANs cableadas es costoso.

En todos estos casos una LAN inalámbrica ofrece una alternativa más efectiva y atractiva. En la mayor parte de estas situaciones, una empresa también dispondrá de una LAN

cableada con servidores y algunas estaciones de trabajo estáticas. Por tanto, una LAN inalámbrica está conectada en muchas ocasiones con una LAN cableada con las mismas premisas, denominándose este campo de aplicación ampliación de redes LAN.

- **Interconexión de edificios**

Otro uso para redes LAN de tecnología inalámbrica es la conexión de redes LANs en edificios vecinos, sean LANs cableadas o inalámbricas. En este caso se usa un enlace no guiado entre dos edificios. Los dispositivos así conectados son generalmente puentes o dispositivos de encaminamiento. Este enlace punto a punto no es en sí mismo una LAN, pero es usual la inclusión de estos sistemas en el contexto de redes LAN inalámbricas.

- **Acceso nómada**

El acceso nómada permite un enlace no guiado entre un centro de LAN y un terminal de datos móvil con antena, como un computador portátil. Un ejemplo es permitir a un empleado que está regresando de un viaje transferir datos desde su computador portátil al servidor en la oficina. También cuando la extensión del medio está fuera del grupo de edificaciones. Los usuarios pueden desplazarse con sus computadores portátiles y conectarse con una LAN inalámbrica desde distintos lugares.

- **Redes ad hoc**

Una red ad hoc es una red par –a-par o *per-to-per* es decir, sin un servidor centralizado configurado temporalmente para reunir algunas necesidades inmediatas. Por ejemplo un grupo de empleados, cada uno con un computador portátil pueden convocarse en un salón de conferencias o una reunión en un salón e clases. Los empleados enlazan sus computadores en una red temporal solo por la duración de la reunión. En este caso la LAN inalámbrica forma una infraestructura estática consistente en una o más celdas con un módulo de control para cada una; dentro de cada celda pueden existir varios sistemas finales estáticos.

Algunos ejemplos o escenarios del uso de las WLANs, donde el uso más frecuente y común es como extensión de redes cableadas:

- Educación: Las instituciones académicas que soportan este tipo de conexión móvil permiten a los usuarios conectarse a la red de la universidad para intercambio de opiniones en las clases, acceder a Internet, etc.
- Corporaciones: Los empleados pueden beneficiarse de una red móvil y podrán acceder a correo electrónico, compartir ficheros, visualizar Webs, independientemente de su ubicación en la oficina.
- Finanzas: Con un computador portátil y un adaptador a la red inalámbrica representantes o ejecutivos pueden tener acceso a una base de datos en tiempo real, enviar y recibir información y aumentar la calidad y velocidad de los negocios. Los grupos de auditorías contables incrementan su eficiencia con una rápida puesta a punto de una red inalámbrica.
- Manufacturación: Las WLANs enlazan las estaciones de trabajo en los diferentes pisos de la fábrica con los dispositivos de adquisición de datos de la compañía.
- Salud: WLAN permite obtener información en tiempo real por lo que permite realizar seguimientos y tratamientos como monitoreo y supervisión de pacientes evitando retardos, errores de transcripción y papeleos.

- Almacenes: Terminales con lectores de códigos de barras y enlaces con redes WLAN, evitan costos de inventarios y tiempos de un conteo físicamente.

C.2. ESTÁNDARES Y PROTOCOLOS.

ESTÁNDAR 802.11

En 1997, IEEE adoptó el estándar IEEE 802.11-1997 para WLANs. Este estándar ha recibido múltiples suplementos, 802.11a, 802.11b, etc. que son los que están disponibles en los equipos de red actuales. En la tabla 1 se presentan todas sus variantes.

El estándar IEEE 802.11 en su edición de 1999 define a la capa física PHY y la capa de control de acceso al medio MAC (Medium Access Control) para una LAN con conectividad inalámbrica.

Define capas físicas PHY para tasas de transmisión de 1 y 2 Mbps en la banda de radiofrecuencia (RF) sin licencia de 2.4 GHz y en la infrarroja (IR). El estándar 802.11 es un miembro de la familia de los estándares 802 emitidos por la IEEE que incluye el 802.3 (Ethernet) y 802.5 (Token ring).

Se amplió dos veces, en 1999 por el 802.11a, que definía la capa física PHY para la banda de 5 GHz a velocidades de 6 hasta 54 Mbps, y por el 802.11b, que definió la capa física PHY para la banda de 2.4 GHz a 5.5 GHz y 11 Mbps.

El propósito del estándar como fue definido por IEEE es "*proveer conectividad inalámbrica a maquinaria automática, equipo, o estaciones que requieren despliegue rápido, que pueda ser portátil o hand-held¹⁵, o pueda estar montado en vehículos que se muevan dentro de un área local.*"

Direcciona FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum), e infrarrojos. La tasa de datos está limitada a 2 Mbps y 1 Mbps para ambos FHSS y DSSS.

FHSS evita el multitrayecto y la interferencia de banda angosta gracias a su esquema de saltos de frecuencia (frequency-hopping). Si un canal está debilitado los demás canales usualmente no lo están, así que los paquetes son enviados a esos saltos donde no se presenta desvanecimiento. FHSS tiene 64 patrones de salto que pueden soportar hasta 15 redes en un mismo lugar. Los sistemas FHSS están limitados a 1 Mbps y opcionalmente 2 Mbps. Típicamente tienen un rango mayor que los sistemas DSSS. FHSS no es compatible con los equipos basados en el estándar 802.11b.

DSSS, como se implementó en 802.11, ocupa 22 MHz del espectro y opera a una tasa de datos de 2 Mbps. DSSS es susceptible al multitrayecto y a la interferencia de banda angosta debido al limitado factor de expansión que usa (solo 11 bits). DSSS solo puede soportar tres canales no interferentes y es compatible con los equipos basados en el estándar 802.11b.

Los equipos basados en 802.11 presentan un buen desempeño en algunas aplicaciones que requieren inmunidad al multitrayecto, que toleran tasas de transmisión bajas y que no

¹⁵ Hace referencia a un dispositivo portable y sostenible en la mano.

desean compatibilidad con los equipos disponibles actualmente, ya que la mayoría de fabricantes de estos dispositivos de red no ofrecen garantía ni servicio técnico para ellos.

Para garantizar la interoperabilidad entre cientos de fabricantes y miles de dispositivos de la familia 802.11 se creó el grupo industrial WECA (Wireless Ethernet Compatibility Alliance), Alianza de Compatibilidad de Ethernet Inalámbrico, encargado de certificar los equipos de sus miembros mediante el Wi-Fi¹⁶ Alliance¹⁰.

Así Wi-Fi es una certificación de interoperabilidad para sistemas 802.11b, que otorga la WECA. El sello Wi-Fi indica que algún aparato ha pasado pruebas independientes y que opera confiablemente con otros equipos certificados en dicha certificación. Los clientes se benefician de este estándar ya que no están atados a la solución de un solo fabricante y pueden comprar puntos de acceso y adaptadores y tarjetas inalámbricas, certificados con Wi-Fi, de diferentes fabricantes y confiar en que trabajarán conjuntamente. Actualmente pertenecen a la WECA más de 250 compañías y se han certificado más de 700 productos.



Figura C.1. Etiqueta Wi-Fi

Fuente: www.wi-fi.org

Según el estándar 802.11, el bloque más elemental de una LAN inalámbrica es un Basic Service Set BSS o conjunto de servicio básico, que consta de varias estaciones de trabajo STAs, ejecutando el mismo protocolo MAC y compitiendo para acceder al medio compartido. Un BSS puede ser aislado, conociéndose entonces como un IBSS, Independent Basic Service Set.

El término *red ad hoc* es usualmente empleado para referirse a un IBSS. Una red ad hoc puede definirse como una red compuesta solamente de estaciones dentro de un rango mutuo en el que la comunicación se realiza haciendo uso de un medio inalámbrico. Una red de este tipo es creada típicamente de manera espontánea y su principal característica es que está limitada en extensión espacial y temporal.

La *red ad hoc* es el primer modo de funcionamiento de una WLAN.

¹⁶ Wireless-Fidelity. Consorcio privado que se encarga de estandarizar los productos WLAN bajo 802.11x.

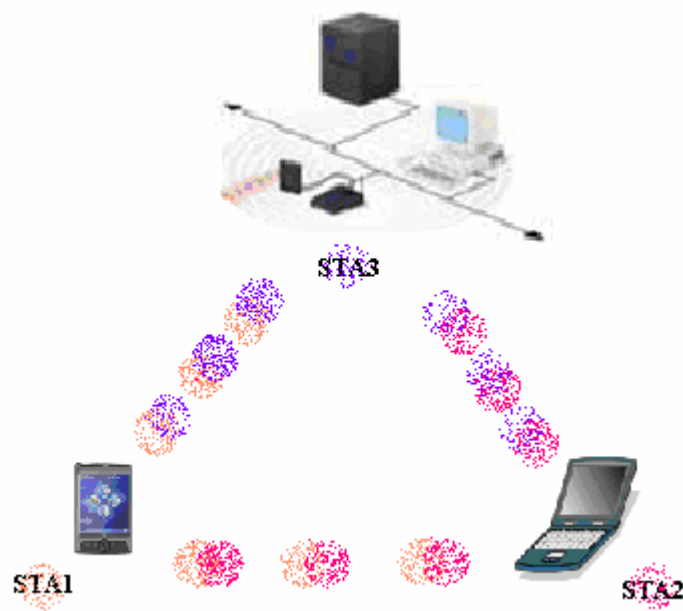


Figura C.2. Modelo red Ad Hoc

Un BSS puede, en lugar de estar aislado, formar parte de una forma de red más extensa compuesta de múltiples BSSs interconectados por un sistema de distribución. En este caso se requiere un punto de acceso AP cuya función es proveer acceso al sistema de distribución. El protocolo MAC puede ser completamente distribuido o controlado por una función de coordinación central localizada en el punto de acceso. El BSS corresponde generalmente con lo que se conoce en la bibliografía como una celda o célula.

El sistema de distribución y los BSSs permiten crear una red de tamaño y complejidad avanzada. IEEE 802.11 se refiere a esta red como un conjunto de servicio extendido ESS, Extended Service Set, el cual consta de dos o más BSSs interconectados por un sistema de distribución. Generalmente, el sistema de distribución es una LAN núcleo cableada. El ESS aparece en el nivel de control de enlace lógico LLC como una única LAN lógica.

Para integrar la arquitectura 802.11 con una LAN cableada tradicional, se introduce un último elemento en la arquitectura: el portal. Un portal es el punto lógico a través del cual se intercambian paquetes entre una red 802.11 y una red cableada (cualquier otra red IEEE 802).

Es posible que un mismo dispositivo ofrezca las dos funciones: AP y portal. Este podría ser el caso cuando el medio de distribución se implementa con componentes IEEE 802.

Los actuales productos y dispositivos inalámbricos ofrecen estas funcionalidades de AP, portal, ruteador e incluso funcionalidades de seguridad y gestión de red.

El segundo modo de operación de las WLANs es en **red infraestructura**, en la cual se incluye el medio de distribución del sistema, uno o más puntos de acceso y cero o más portales. En una red infraestructura se encuentran las funciones de distribución e integración de un ESS.

La **Figura C.3.** muestra el modelo de una red infraestructura:

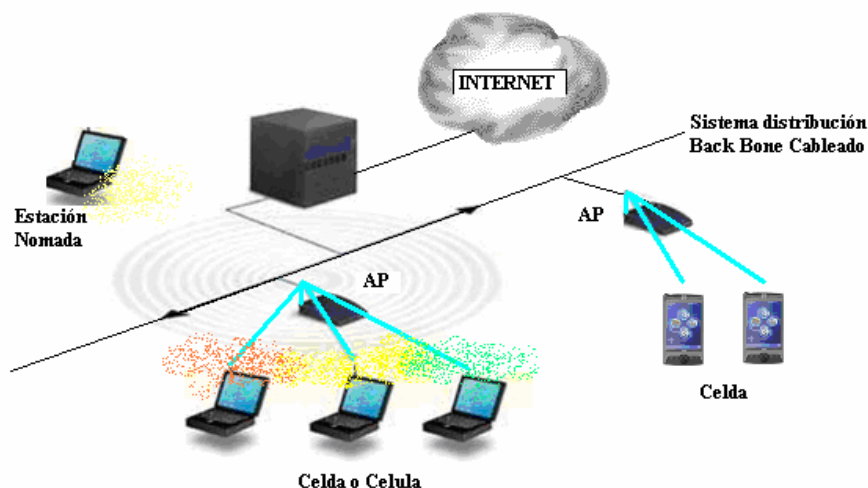


Figura C.3. Modelo red Infraestructura

La capa física PHY.

La especificación del FHSS de 2.4 GHz, y la especificación IR original del 802.11 normalmente no se usan. El rango limitado que es de aproximadamente 15 metros del OFDM 5GHz para PHY lo hacen menos atractivo para la mayoría de los usuarios. Actualmente la mayoría de los productos implementan la tecnología DSSS del 802.11b para una velocidad de transmisión de datos de 11 Mbps por su ventaja de precio/desempeño. Debido a que las otras PHY son raramente usadas, el resto de este documento asume que se está usando 2.4 GHz DSSS PHY.

La Capa de Control de Acceso al Medio MAC.

Mientras que la PHY es diferente que la del 802.3 Ethernet, la especificación MAC es similar a la especificación MAC del 802.3 Ethernet además del 802.2 LLC Logical Link Control, que hace el espacio de la dirección MAC del 802.11 compatible en con aquel de los otros protocolos 802. Mientras que la MAC de Ethernet 802.3 es esencialmente Carrier Sense Multiple Access / Collision Detection (CSMA/CD), la MAC del 802.11 es Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA). La razón para esta diferencia es que no existe un modo práctico para transmitir y recibir al mismo tiempo en el medio inalámbrico WM. Como el nombre lo implica CSMA/CA intenta evadir colisiones en WM colocando información de duración en cada frame MAC, de tal forma que las estaciones receptoras puedan determinar cuánto tiempo deberá permanecer el frame en WM. Si la duración del frame MAC previo ha expirado y una revisión rápida del WM muestra que no está ocupado, se le permite transmitir a la estación emisora. De esta forma, es un esfuerzo coordinado, diferente a aquel de CSMA/CD, que permite a un emisor transmitir en cualquier momento que el medio no esté demasiado ocupado.

ESTÁNDAR 802.11A

El estándar 802.11a opera en las tres sub-bandas de la banda de 5 GHz (5150 - 5250, 5250 - 5350 y 5470 - 5725) y por esta razón no es compatible con 802.11b. Las sub-

bandas están designadas según la aplicación. La primera está especificada para uso indoor¹⁷ exclusivamente, la segunda está designada para uso indoor y outdoor¹⁸ y la tercera está designada para uso outdoor exclusivamente.

La interferencia de radio frecuencia RF es baja debido a que la banda de 5 GHz es menos utilizada que las otras bandas de frecuencia libre, como la de 2.4 GHz. Cada una de las sub-bandas de 5 GHz tienen cuatro canales separados que no se superponen. Estos emplean OFDM, Orthogonal Frequency Division Multiplexing usando 52 subportadoras para evitar la interferencia y el multitrayecto, soportan una tasa máxima de datos de 54 Mbps usando 64 QAM, Quadrature Amplitude Modulation y permiten tasas de transmisión de 6, 12 y 24 Mbps. El protocolo especifica las sensibilidades mínimas de recepción en un rango de -65 dBm para una velocidad de 54 Mbps a -82 dBm para una velocidad de 6 Mbps. Según los vendedores de puntos de acceso 802.11a, cada AP puede llegar a soportar alrededor de 256 estaciones.

ESTÁNDAR 802.11B

Es el protocolo estándar más ampliamente usado, 802.11b requiere tecnología DSSS, especifica una tasa máxima de datos de 11 Mbps y un esquema para reducir a una tasa menor cada vez que las tasas altas no se puedan mantener. Este protocolo soporta tasas de transmisión de 11 Mbps, 5.5 Mbps, 2 Mbps y 1 Mbps usando DSSS y CCK, Complementary Code Keying.

El estándar 802.11b usa CCK como el esquema de modulación que le permite alcanzar las tasas de 5.5 Mbps y 11 Mbps. 802.11b redujo el factor de expansión de 11 bits (empleado en 802.11) a 8 bits para alcanzar tasas más altas. El esquema de modulación compensa la pérdida de ganancia por el procesamiento a causa de la disminución del factor de expansión con una mayor corrección de errores.

La especificación 802.11b permite a las transmisiones inalámbricas de aproximadamente 11 Mbps alcanzar distancias de hasta 100m a puertas cerradas y de hasta 300m en ambientes abiertos en conexiones punto a punto en la banda de los 2.4 GHz. Estas distancias dependen de los obstáculos en la trayectoria, de los materiales y de si hay o no línea de vista. Según los vendedores de puntos de acceso con este estándar, cada AP puede soportar alrededor de 32 estaciones.

Respecto a la capacidad compartida del canal, debido a que la capacidad de transmisión está limitada por las características del medio en el cual se desenvuelve la aplicación y la distancia del cliente al punto de acceso AP, la WLAN se configura de modo automático por defecto, para que se regule según la calidad del enlace. Además dicha capacidad puede ser compartida por varios usuarios usando el mismo punto de acceso AP. Así cuando la capacidad no es suficiente para cada usuario debido a multiplicidad de usuarios por ejemplo, se hace necesario utilizar más puntos de acceso en una celda para aumentar el tráfico.

Cuando se utiliza el mismo tiempo para la comunicación, la norma IEEE 802.11 dice que se debe dejar una separación de 22 MHz entre las frecuencias centrales de los canales. Con esta norma se pueden tener hasta tres canales para 802.11b, es decir, se puede tener hasta tres puntos de acceso trabajando en una misma celda o área de cobertura programados en canales diferentes sin que se presenten interferencias de radiofrecuencia.

¹⁷ Se refiere a las aplicaciones inalámbricas en interiores o espacios cerrados como oficinas, edificios, etc.

¹⁸ Se refiere a las aplicaciones inalámbricas en exteriores o espacios abiertos.

Se recomienda programar los puntos de acceso cada cinco canales, es decir, si se trabaja con tres puntos de acceso se deben programar en los canales 1, 6 y 11 respectivamente, o se puede en los canales 2, 7, y 12 respectivamente. Para la norma 802.11a, se pueden tener hasta ocho puntos de acceso trabajando en la misma celda.

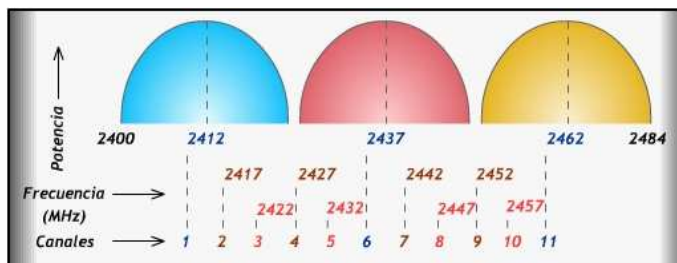


Figura C.4. Distribución de canales en la banda 2.4 GHz

ESTÁNDAR 802.11G

El estándar 802.11g es una extensión del 802.11b y opera en la banda de 2.4 GHz. 802.11g incrementa la tasa de transmisión de datos de 802.11b a 54 Mbps usando la misma tecnología OFDM que utiliza 802.11a. El rango a 54 Mbps es más bajo que el de los APs de 802.11b que operan a 11 Mbps. Como resultado, si una celda 802.11b es actualizada a 802.11g, las tasas de transmisión altas no estarán disponibles a través de toda el área. Probablemente será necesario aumentar el número de APs y dividir las celdas existentes en celdas más pequeñas.

802.11g ofrece una velocidad de transmisión más alta y mayor tolerancia al multitrayecto que 802.11b. A pesar de que existe mayor interferencia en la banda de 2.4 GHz, 802.11g es un estándar con una buena combinación entre rango y ancho de banda, además es compatible con los equipos que se rigen por el estándar 802.11b.

La **Tabla C.2.** describe las variaciones o diferentes versiones que se han publicado respecto al Estándar 802.11, desde la versión 802.11a, 802.11b, c, d, e, f, g, h, y 802.11i y 802.11x.

802.11	DESCRIPCIÓN
802.11a	Estándar para WLAN que opera en la banda de 5 GHz. Tasa de transmisión hasta 54 Mbps. Publicado en 1999.
802.11b	Estándar conocido como Wi-Fi. Banda de 2.4 GHz. Hasta 11 Mbps. Publicado en 1999.
802.11c	Informa de procedimientos MAC específicos de 802.11 a la ISO / IEC ¹⁹
802.11d	Publicación de requerimientos y definiciones de 802.11 para países que aun no lo tienen.
802.11e	Intento de mejorar la MAC de 802.11 para aumentar QoS. ²⁰
802.11f	Tiene como propósito incrementar la compatibilidad de puntos de acceso APs de diferentes fabricantes.
802.11g	Extensión de 802.11b para aumentar la tasa de transmisión a 54 Mbps

¹⁹ ISO / IEC. Organización Internacional para la Estandarización / Comisión Electrotécnica Internacional.

²⁰QoS. Quality of Service. Calidad de Servicio.

	operando en la banda de 2.4 GHz. Publicado en 2003.
802.11h	Mejora la MAC 802.11 y la PHY 802.11a para proveer administración de la red y extensión de control del espectro y la potencia transmitida.
802.11i	Mejora los mecanismos de seguridad y autenticación de 802.11.
802.11x	Mejoramiento de la seguridad en las redes 802.11b.

Tabla C.2. Variantes de 802.11

C.3. SEGURIDAD.

Los sistemas inalámbricos por naturaleza son inseguros debido a que la información viaja a través del aire, estando disponible para cualquier persona que se encuentra dentro del área de cobertura de la WLAN. Se debe tener presente que el área de cobertura, supere las dimensiones físicas de la habitación o edificación que la contiene, el área de cobertura no posee límites definidos. Con el equipo adecuado, un intruso puede ingresar a la red, consumiendo ancho de banda y recursos que deterioran su rendimiento.

El problema se agrava aún más cuando la WLAN forma parte de una red corporativa, ya que abre un espacio por el cual un usuario mal intencionado puede saltarse los sistemas tradicionales de seguridad, por ejemplo un *firewall*, ingresando al *backbone* principal de la red, teniendo acceso a los principales y elementos y equipos activos que forman la red como los servidores, routers, y estaciones de trabajo. Para solucionar estos inconvenientes de seguridad, en la red LAN se deben implementar los sistemas de seguridad propios de las redes WLAN, complementados con sistemas de seguridad tradicionales, tal como:

- SSID: Service Set IDentification.
- WEP: Wired Equivalent Privacy.
- Autenticación Shared Key.
- WPA: Wi-Fi Protected Access .
- Filtrado de direcciones MAC.
- Firewall entre el AP y el backbone de la red.
- Redes Privadas Virtuales (VPN).
- Autenticación 802.1x y EAP

Los sistemas de seguridad inalámbricos deberán detener a cualquier usuario no autorizado, ya que no conocerá las claves de acceso a la red y tampoco estará presente en la tabla de direcciones MAC que el AP contiene. Si estos son violados, el intruso tendrá acceso a los servicios de la red WLAN, pero no podrá acceder a la red principal, el firewall lo detendrá.

- **SSID (Service Set ID).** El SSID es una cadena usada para definir un dominio de cobertura común entre múltiples puntos de acceso. Diferentes SSIDs en los APs puede permitir redes inalámbricas traslapadas. El SSID se creó para ser una clave básica sin la cual ningún cliente podría conectarse a una red, sin embargo, esta seguridad puede ser fácilmente violada si los puntos de acceso no tienen deshabilitada la opción de difundir su SSID a través de mensajes broadcast que se envían múltiples veces por segundo, ya que con cualquier herramienta de análisis de tráfico pueden ser vistos haciendo que la clave sea de conocimiento público.

El SSID debe ser cambiado periódicamente en cualquier WLAN, ya que evita que otras personas usen la red sin autorización.

- **WEP (Wired Equivalent Protocol).** El estándar 802.11b también definió un método de autenticación y cifrado llamado WEP para aliviar las preocupaciones en materia de seguridad. Generalmente, la autenticación es utilizada para evitar accesos no autorizados a la red, mientras que el cifrado es usado para frustrar a intrusos que traten de interpretar las transmisiones capturadas. El cifrado WEP está basado en RC4, un algoritmo que usa una clave de 40 bits (que cuenta con un vector de inicialización con 24 bits aleatorios) para cifrar datos de transmisiones inalámbricas. De estar habilitado el cifrado, la misma clave WEP debe ser usada en todos los clientes y puntos de acceso para que exista comunicación. Algunos vendedores ofrecen 128-bit WEP, lo cual hace más difícil para los intrusos descifrar las transmisiones; sin embargo esta variante no está definida por el estándar y los productos que la usen pueden no ser interoperables entre sí.
- **Autenticación Shared Key. Clave Compartida de autenticación.** Para prevenir el acceso no autorizado, WEP define un protocolo de autenticación. El estándar 802.11b define dos formas de autenticación: sistema abierto y clave compartida. En el sistema abierto cualquier cliente puede asociarse con el punto de acceso sin pasar por el proceso de autenticación. No hay autenticación de clientes ni cifrado de datos. En sistemas con clave compartida, el AP envía una “frase de reto” al cliente que solicita autenticación. El cliente cifra la frase de reto usando la clave compartida y la devuelve al AP. Si el AP puede descifrar el mensaje y recuperar la frase transmitida comprueba que el cliente posee la clave correcta y le permite conectarse a la red. Debe observarse que si la frase de reto y la respuesta del cliente están disponibles en el medio, un pirata de red o los afamados *hackers* pueden obtener la clave WEP. Según esto, las autenticaciones de sistema abierto y de clave compartida no son seguras y por esto se han implementado otros mecanismos de seguridad.
- **Filtrado de direcciones MAC.** Además de los dos mecanismos mencionados propuestos por el estándar 802.11, algunas compañías implementan filtrado de direcciones MAC en sus productos. El filtro de direcciones MAC contiene las direcciones MAC de las tarjetas de interfaz de red inalámbrica que pueden asociarse con un punto de acceso dado. Un filtro de direcciones MAC no es tampoco un sistema de seguridad confiable, ya que con un analizador de tráfico de red pueden descubrirse fácilmente las direcciones MAC autorizadas para conectarse. Así que usando los controladores del adaptador inalámbrico (disponibles en Internet para la mayoría de marcas) puede configurarse en la tarjeta la dirección MAC capturada y ganar acceso a la red. A pesar de su vulnerabilidad, el filtrado de direcciones MAC dificulta aún más el acceso para clientes no autorizados.
- **Wi-Fi Protected Access (WPA).** Este estándar fue presentado en noviembre de 2002 por la alianza Wi-Fi y se espera que remplace el estándar actual WEP que está disponible con los equipos Wi-Fi. WPA usa un protocolo de integridad de clave temporal TKIP (Temporal Key Integrity Protocol), un esquema de seguridad llamado Key Mix y un chequeo de integridad del mensaje MIC (Message Integrity Check). TKIP también utiliza un protocolo de reasignación de clave rápido que cambia la clave de cifrado después de más o menos 10000 paquetes.

Idealmente WPA trabajará con servidores de autenticación (ASs) y requerirá del apoyo de 802.11x y EAP, los cuales le permiten a un adaptador cliente negociar a través de un AP con un AS usando transacciones cifradas para cambiar las claves de cada sesión.

- **Redes Privadas Virtuales (VPNs).** Una VPN permite a un grupo de usuarios específico acceder a los datos y recursos de una red privada de forma segura en Internet o en otras redes. Las VPNs se caracterizan por el uso de túneles, cifrado, autenticación y control de acceso sobre una red pública. Una VPN crea conexiones virtuales entre dos estaciones a través de un túnel, el cual actúa como un conducto que conecta dos puntos de una red. Iniciado típicamente por un usuario remoto, el proceso de tunneling encapsula los datos en paquetes TCP/IP que pueden viajar seguros en Internet hasta un servidor VPN en el receptor, donde son descifrados y desencapsulados en la red LAN privada.

Para implementar una VPN en una WLAN 802.11, debe desarrollarse una aplicación cliente de software en todas las máquinas que usen la WLAN e introducir una puerta de enlace VPN en la red, entre el AP y los demás dispositivos de la WLAN.

Se debe construir un túnel entre la estación con el adaptador inalámbrico y un servidor VPN, de tal forma que todo el tráfico que pase por el AP pase por la puerta de enlace (y a través de ella al servidor VPN) antes de entrar a la LAN. Los datos ya desencapsulados en el servidor pueden viajar libremente hacia su destino, al otro lado del túnel, en el interior de la LAN. Un túnel VPN provee autenticación, confidencialidad e integridad de los datos, haciendo innecesarios otros mecanismos de seguridad como WEP.

- **Firewall entre el AP y el backbone de la red.** Se puede implementar a través de un equipo dedicado como firewall o configurar desde el entorno de configuración propio de los APs que tienen esta característica. Generalmente los APR, Access Point Router presentan esta opción de configuración de seguridad.

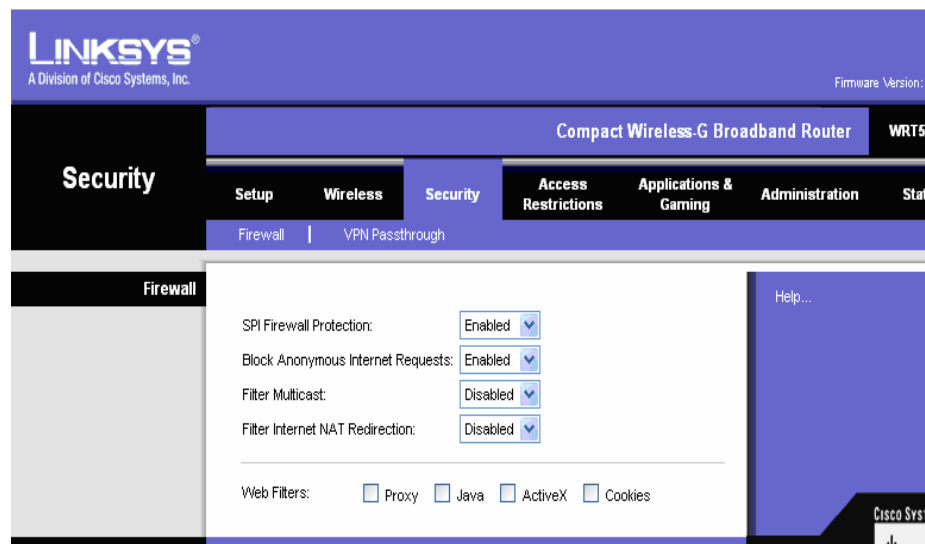


Figura C.5. Panel de Configuración de Seguridad Firewall en un APR Linksys

En la figura arriba vemos las múltiples opciones que nos brinda un APR 54g de Linksys en cuanto a la seguridad firewall. Nos permite elecciones de protección

firewall SPI, bloques anónimos de requerimientos de Internet, filtrado multicast, filtro Internet de redireccionamiento NAT; así como la posibilidad de habilitar o deshabilitar filtros Web a Proxy, Java, ActiveX y cookies.

- **Autenticación 802.1x y EAP.** 802.1x permite que un usuario sea autenticado por una autoridad central. Existen múltiples algoritmos que se pueden emplear para determinar si un cliente es auténtico, así que se pueden encontrar soluciones basadas en certificados, basadas en claves de acceso, basadas en tarjetas inteligentes o soluciones híbridas, que combinan certificados y claves de acceso. 802.1x usa EAP (Extensible Authentication Protocol), un protocolo (RFC 2284) que trabaja sobre Ethernet, Token Ring, o WLANs para el intercambio de mensajes durante el proceso de autenticación.

La autenticación 802.1x para WLANs tiene tres componentes principales: el solicitante (usualmente el software del cliente), el autenticador (usualmente el AP) y el AS que es usualmente un servidor RADIUS²¹ aunque este tipo de servidor no es requisito en 802.1x. Un servidor RADIUS puede realizar consultas en una base de autenticación local si esto es lo adecuado para el escenario, o bien la solicitud puede transmitirse a otro servidor para su validación. Cuando RADIUS decide que se puede validar al equipo en esa red vuelve a enviar el mensaje al punto de acceso y este permite el flujo de datos hacia la red.

Este autenticador se conecta a la red LAN. El flujo normal para una autenticación 802.1x es como sigue: El solicitante trata de conectarse al AP enviando un mensaje de inicio. El AP detecta al solicitante y habilita el puerto del solicitante en un estado “no autorizado” en el que solo se permiten mensajes 802.1x/EAP y se bloquea cualquier otro tipo de tráfico. El solicitante envía un mensaje EAP de inicio, al cual el AP contesta con una solicitud de identidad. El paquete EAP de respuesta que envía el cliente revelando su identidad es enviado al AS, el cual autentica al solicitante y responde aceptándolo o rechazándolo. Dependiendo de la respuesta del AS, el AP habilita o mantiene bloqueado el puerto del solicitante. Este esquema de autenticación mediante el servidor RADIUS se ilustra en la siguiente figura: **Figura C.6.**

El inconveniente que presenta 802.1x/EAP es la falta de soporte para los solicitantes en la mayoría de sistemas operativos, solo tienen soporte Windows XP y Windows 2000 y hasta que este problema no sea resuelto, 802.1x no podrá proveer una solución completa al problema de seguridad.

²¹ RADIUS (Remote Authentication Dial-In User Service), su especificación se puede consultar en la RFC 2058.

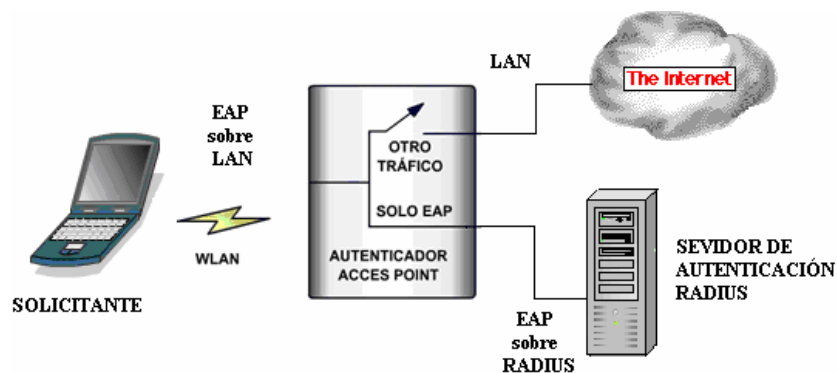


Figura C.6. Autenticación 802.1x y servidor RADIUS

Sistema de administración

El sistema de administración es aquel que provee los servicios necesarios para que el usuario utilice la red en forma cómoda y segura. Algunos servicios administrativos son:

- Asignación dinámica de direcciones de red, mediante servidor DHCP.
- Acceso a la red principal, a través de un Router.
- Protección de la red con un firewall.

Algunos dispositivos inalámbricos, APs y routers, cuentan con la capacidad de prestar estos servicios. Por ejemplo productos ofrecidos por Linksys²² brindan todas estas características en un solo dispositivo, con funcionalidades administrativas y de gestión muy robustas. Una alternativa, es implementar una máquina externa con los servicios necesarios para realizar la gestión de la red.

Existe un sin número de herramientas, tanto propietarias como de distribución libre que nos permiten la administración y gestión de la red inalámbrica, en las cuales se puede hacer monitoreo de tráfico y administración de seguridad. Las herramientas más conocidas y que podemos obtener gratis en la Web están mencionadas en el ANEXO H.

²² Linksys es una filial de Cisco, encargada del wireless networking al Home Level y SMB.

ANEXO D. OTRAS TECNOLOGIAS INALÁMBRICAS

D.1. TECNOLOGÍA HOMERF 2.0

Este estándar europeo se enfoca principalmente hacia aplicaciones residenciales, funciona en la banda de 2.4 GHz. HomeRF 2.0 puede operar a tasas de hasta 10 Mbps y permite integrar voz y datos en un amplio rango de dispositivos como PCs, PDAs, teléfonos inalámbricos, etc.

Dentro de sus características se encuentran que utiliza TDMA, Time Division Multiple Access y CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) a nivel de capa MAC y FHSS con una frecuencia de 50 saltos por segundo, a nivel de capa física. Su máxima potencia de transmisión es de 24 dBm y su rango de cobertura de hasta 100 m con línea de vista directa.

Con una finalidad muy similar, la tecnología HomeRF, basada en el protocolo de acceso compartido SWAP Shared Wireless Access Protocol, encamina sus pasos hacia la conectividad sin cables dentro del hogar para transportar voz y datos.

Los principales veedores de estos sistemas, se agrupan en torno al Consorcio que lleva su mismo nombre HomeRF, teniendo a Proxim (una filial de Intel) como el miembro que más empeño esta realizando en la implantación de dicho estándar. Además de la sombra de Intel, Compaq es otra de las firmas relevantes que apoya el desarrollo de productos HomeRF. El soporte a esta tecnología se materializa en que actualmente ambas significativas firmas poseen cada una de ellas un producto bajo esta novedosa configuración. Al igual que WECA o Bluetooth SIG, el HRFWG HomeRF Working Group, es un grupo compañías encargadas de proporcionar y establecer un cierto orden en este océano tecnológico, obligando que los productos fabricados por las empresas integrantes de este grupo tengan una buena interoperatividad. Por si toda esta competitividad no fuera suficiente, el ETSI, Instituto de Estándares de Telecomunicaciones Europeo es otra de las reconocidas organizaciones de estandarización, culpable, entre otros, de haber desarrollado el estándar GSM para la telefonía celular digital.

D.2. TECNOLOGÍA HIPERLAN2

HiperLAN2, High Performance Radio LAN es una especificación inalámbrica desarrollada dentro del proyecto de redes de acceso de radio de banda ancha, BRAN del ETSI durante los años 1991 y 1996 en el cual su objetivo primordial era conseguir una tasa de transferencia mayor que la ofrecida por la especificación IEEE 802.11 y propuesta con el fin de proveer acceso de banda ancha sobre una variedad de redes como redes móviles de tercera generación 3G, redes ATM y redes basadas en IP como las WLANs. Permite tasas de datos de hasta 54 Mbps para comunicaciones inalámbricas de corto alcance, hasta 150 metros en ambientes de interior (indoor) y de exterior (outdoor), en las bandas de 5150 a 5300 MHz y de 5470 a 5725 MHz.

Según los estudios realizados, HyperLAN incluía cuatro estándares diferentes, de los cuales el denominado Tipo 1, es el que verdaderamente se ajusta a las necesidades futuras de las WLAN, estimándose una velocidad de transmisión de 23,5 Mbps, notablemente superior a los 1 ó 2 Mbps de la normativa IEEE 802.11b. Actualmente, el ETSI dispone

de la especificación HiperLAN2 que mejora notablemente las características de sus antecesoras, ofreciendo una mayor velocidad de transmisión en la capa física de 54 Mbps para lo cual emplea el método de modulación OFDM (Orthogonal Frequency Digital Multiplexing) y ofrece soporte QoS. Bajo esta especificación se ha formado un grupo de reconocidas firmas el HiperLAN2 Global Forum H2GF, con la intención de sacar al mercado productos basados en este competitivo estándar. HiperLAN2 posee algunas similitudes con el estándar 802.11a, al igual que este utiliza modulación OFDM y opera en la banda de frecuencias de 5 GHz, sin embargo los sistemas tecnológicos para el control de acceso son diferentes. Mientras 802.11a utiliza CSMA-CA, HiperLAN2 usa TDMA.

El estándar HiperLAN2 es más difícil de implementar que su análogo, el 802.11a por lo que muy pocos dispositivos se ciñen a él, incluso, algunos autores lo consideran prácticamente muerto.

D.3. TECNOLOGÍA WI-MAX.

A pesar de que el proyecto para la creación de un nuevo estándar se gestó hace más de seis años en el IEEE, fue hasta abril de 2002 que la primera versión del mismo, la 802.16, se publicó, y se refería a enlaces fijos de radio con línea de vista (LoS) entre transmisor y receptor, pensada para cubrir la "última milla" (o la primera, según desde que lado se mire), utilizando eficientemente varias frecuencias dentro de la banda de 10 a 66 GHz.

En marzo de 2003, se ratificó una nueva versión, el 802.16a, y fue entonces cuando WiMAX, como una tecnología de banda ancha inalámbrica, empezó a cobrar relevancia. También se pensó para enlaces fijos, pero llega a extender el rango alcanzado desde 40 a 70 Km, operando en la banda de 2 a 11 GHz, parte del cual es de uso común y no requiere licencia para su operación. Es válido para topologías punto a multipunto y, opcionalmente, para redes en malla, y no requiere línea de visión directa. Emplea las bandas de 3,5 GHz y 10,5 GHz, válidas internacionalmente, que requieren licencia (2,5-2,7 en Estados Unidos), y las de 2,4 GHz y 5,725-5,825 GHz que son de uso común y no requieren disponer de licencia alguna.

Un aspecto importante del estándar 802.16x es que define un nivel MAC que soporta múltiples enlaces físicos PHY. Esto es esencial para que los fabricantes de equipos puedan diferenciar sus productos y ofrecer soluciones adaptadas a diferentes entornos de uso. Pero Wi-Max también tiene competidores, y así una alternativa es el estándar *Hiperaccess* (>11 GHz) e *HiperMAN* (<11 GHz) del ETSI, pero el auge que está tomando Wi-Max ha hecho que se esté estudiando la posibilidad de armonizarlo con esta última norma, que también utiliza una modulación OFDM. Sin olvidarnos de *Mobile-Fi*, el estándar 802.20 del IEEE, específicamente diseñado desde el principio para manejar tráfico IP nativo para un acceso móvil de banda ancha, que provee velocidad entre 1 y 16 Mbps, sobre distancias de hasta 15 o 20 Km, utilizando frecuencias por debajo de la banda de 3,5 GHz.

Estas velocidades tan elevadas se consiguen gracias a utilizar la modulación OFDM (Orthogonal Frequency División Multiplexing) con 256 subportadoras, la cual puede ser implementada de diferentes formas, según cada operador, siendo la variante de OFDM empleada un factor diferenciador del servicio ofrecido. Esta técnica de modulación es la que también se emplea para la TV digital, sobre cable o satélite, así como para Wi-Fi (802.11b) por lo que está suficientemente probada. Soporta los modos FDD y TDD para facilitar su interoperabilidad con otros sistemas celulares o inalámbricos.

Soporta varios cientos de usuarios por canal, con un gran ancho de banda y es adecuada tanto para tráfico continuo como a ráfagas, siendo independiente de protocolo; así, transporta IP, Ethernet, ATM etc. y soporta múltiples servicios simultáneamente ofreciendo Calidad de Servicio QoS en 802.16e, por lo cual resulta adecuado para voz sobre IP (VoIP), datos y vídeo. Otra característica de WiMAX es que soporta las llamadas antenas inteligentes (smart antenas), propias de las redes celulares de 3G. Estas antenas inteligentes emiten un haz muy estrecho que se puede ir moviendo, electrónicamente, para enfocar siempre al receptor, con lo que se evitan las interferencias entre canales adyacentes y se consume menos potencia al ser un haz más concentrado.

También, se contempla la posibilidad de formar redes malladas (mesh networks) para que los distintos usuarios se puedan comunicar entre sí, sin necesidad de tener visión directa entre ellos. Ello permite, por ejemplo, la comunicación entre una comunidad de usuarios dispersos a un coste muy bajo y con una gran seguridad al disponerse de rutas alternativas entre ellos. Así, Wi-Max puede resultar muy adecuado para unir hot spots Wi-Fi a las redes de los operadores, sin necesidad de establecer un enlace fijo. El equipamiento Wi-Fi es relativamente barato pero un enlace E1 o DSL resulta caro y a veces no se puede desplegar, por lo que la alternativa radio parece muy razonable. Wi-Max extiende el alcance de Wi-Fi y provee una seria alternativa o complemento a las redes 3G, según como se mire.

Para las empresas, es una alternativa a contemplar, ya que el coste puede ser hasta 10 veces menor que en el caso de emplear un enlace E1 o T1. En Colombia la ciudad de Cali, después de Bucaramanga está ingresando en el uso de esta tecnología para uso residencial y se espera que las principales ciudades del país adopten este servicio.

	Wi-Fi	Wi-Max	HomeRF	HyperLAN2
Velocidad	11-54 Mbps	124 Mbps	10 Mbps	54 Mbps
Cobertura	300 m	40-70 Km	100 m	150 m
Licencia	No	Si/No	No	No
Ventajas	Velocidad y Precio	Velocidad y Alcance	Velocidad	Velocidad
Método acceso	CSMA	CSMA	CSMA/CA TDMA	TDMA
Desventajas	Bajo alcance	Interferencias?	Poco alcance y compatibilidad	Poco alcance y compatibilidad

Tabla D.1. Comparación 802.11b con otras tecnologías.

ANEXO E. REQUERIMIENTOS DE DISEÑO DE UNA WLAN Y MÉTODO ESTUDIO DE SITIO (SITE SURVEY)

REQUERIMIENTOS DE DISEÑO.

Es muy importante definir los requerimientos al comienzo de un proyecto. Si esto no se realiza probablemente no se instalará una solución que reúna completamente las necesidades de los usuarios o que sea compatible con los otros sistemas existentes. Es necesario tener esto claro y presente porque resultaría difícil y costoso y, en algunos casos inviable hacer una nueva labor de rediseño y de reingeniería una vez la solución esta implementada.

Una WLAN debe tener la misma clase de requerimientos típicos de una LAN, incluyendo alta capacidad, habilidad para cubrir distancias cortas, conectividad completa entre estaciones enlazadas y capacidad de transmisión.

Los requerimientos definen las bases del diseño como decisiones técnicas de cuál tecnología WLAN se debe elegir, la cual define que componentes que se debe usar y como la solución trabajará. Revisaremos los requerimientos más comunes acorde al diseño a implementar.

- **Arquitectura.** Una descripción de la arquitectura para la fácil ubicación y desempeño de los dispositivos que incluye planos de los pisos o edificaciones, el tipo de construcción, y posibles ubicaciones de los puntos de acceso APs. Hay que considerar hacer dibujos de los edificios y caminar a través de ellos para verificar la exactitud. También se hace necesario tomar fotos a los edificios que tienes varios pisos. Adicionalmente una inspección visual para completar esta valoración. Todo esto ayudará a capturar el medio para tomar las alternativas correctas de diseño.
- **Aplicaciones.** Últimamente las WLANs deben soportar aplicaciones de usuarios, luego hay que definir las completamente. Estas aplicaciones podrían ser aplicaciones generales de oficina como navegación y búsqueda en la Web, correo electrónico y transferencia de archivos. Podrían ser aplicaciones como monitoreo inalámbrico de pacientes en un hospital o consulta y envío de precios en un almacén. Hay que especificar los tipos de información como voz, datos y video y como se transmitirán a través de la facilidad. Los requerimientos de las aplicaciones permiten especificar el flujo de datos y la velocidad de transmisión cuando se diseñe el sistema.
- **Usuarios.** No hay que olvidar el número de usuarios y dónde ellos usarán la WLAN. Es importante identificar si los usuarios serán usuarios móviles o usuarios estacionarios, lo cual provee una base para incluir roaming²³ en el diseño. Los usuarios móviles se moverán a través de la locación y posiblemente vagarán a través de dominios IP, creando la necesidad de manejar

²³ Capacidad de un dispositivo para moverse entre zona de cobertura sin interrumpir el servicio ni perder conectividad

direccionamiento IP dinámico. Algunos usuarios serán estacionarios tales como computadores de escritorio con tarjetas inalámbricas PCI.

- **Áreas de Cobertura.** Esto describe donde los usuarios necesitarán acceso a la WLAN. Los usuarios pueden necesitar conectividad solo en las oficinas o en los cuartos de conferencia, pero también deben estar habilitados en otras áreas sin conectividad inalámbrica como la cafetería. La especificación correcta del área de cobertura evitará gastos innecesarios de instalación de puntos de acceso donde no son necesitados. De manera obvia y tácita, también el área de cobertura determina la región o país donde la WLAN operará y esto tiene efectos en la planeación de los canales y en la disponibilidad de los productos inalámbricos a escoger y en el uso o no de licencias. Las distancias típicas de un WLAN tienen diámetro de 100 a 300 m.
- **Seguridad.** Describe la sensibilidad de la información siendo almacenada y enviada sobre la WLAN. En este parámetro de diseño se establece la necesidad de encriptación si los usuarios van a transmitir información tal como números de tarjetas de crédito. Hay que asegurarse de incluir protección contra ‘espías’ incluyendo requerimientos personales de firewall. Dar completa y abundante seguridad conciente que el diseño a realizar protegerá la información valiosa y confidencial de la institución o compañía.
- **Dispositivos finales de usuario.** Se deben especificar los dispositivos finales de usuario, como el hardware y el sistema operativo, para asegurar que la solución se acomoda a estos. Por ejemplo se puede especificar que los usuarios finales tendrán computadores portátiles IBM corriendo con WindowsXP Professional, o una marca particular de computadores de bolsillo teniendo WindowsCE con interfaces CompactFlash. Esto da una base para decidir que tipo de tarjetas NIC 802.11 se usarán, tan bien como la valoración de dispositivos intermedios.
- **Vida y duración de las baterías.** Una tarjeta NIC 802.11 consumirá un par de cientos de miliamperios. Las baterías bajo esta carga durarán desde un par de horas a un día o más, dependiendo del tamaño de la batería. Hay restricciones para la mayoría de las aplicaciones, pero esto es benéfico para la cantidad de vida de la batería que los usuarios realmente necesitarán. Esta información se puede utilizar para decidir si se activa o implementa un administrador de energía, especificar las baterías grandes o determinar un plan efectivo de carga de baterías.
- **Sistema de interfaces.** En la mayoría de los casos los usuarios necesitarán acceder a información ubicada en servidores que están en la parte cableada del sistema. Por ejemplo se puede encontrar que los usuarios necesitarán interfaces con el sistema de administración IBM AS/400.
- **Financiación.** En el escenario de los requerimientos es necesario preguntar cuánto dinero hay disponible. Si el presupuesto o el límite de los fondos es conocido, se sabrá con cuanto dinero se trabajará en la solución. En la mayoría de los casos, como siempre, la compañía o institución preguntará el costo del sistema. Se hace necesario entonces definir los requerimientos y diseñar el sistema antes de dar un costo estimado.

- **Cronograma.** Las compañías o los ‘clientes’ siempre quieren tener su red WLAN instalada y en operación lo antes posible y en el menor tiempo. Se necesita hacer un compromiso con las fechas reales de terminación de acuerdo a un plan establecido y a los requerimientos y necesidades inmediatas o venideras de la organización. Por ejemplo aplicaciones que serán utilizadas en una época comercial como navidad, en almacenes y tiendas.

Después de definir estos elementos, se debe tener la suficiente información para diseñar la solución. Antes de proceder se debe estar seguro de tener claros todos estos requerimientos, sino se puede considerar la posibilidad de hacer algún prototipo o una prueba piloto antes de gastar mucho dinero en el diseño y en la instalación. También hay que tener en cuenta procedimientos de control de cambios, para mantener todo bajo control de manera que la meta del proyecto no se torne en algo que no se pueda abordar, algo muy costoso o algo que aún no se necesite.

MÉTODO ESTUDIO DE SITIO (SITE SURVEY).

Site Survey quiere decir *Análisis del Lugar*. Es una metodología utilizada en muchas áreas como en estudios y estructuras demográficas, donde mediante encuestas los entrevistadores deben seguir un recorrido determinado, estrategia geográfica dada por un *site survey* en la zona donde se tomará la muestra estadística. Se puede decir que el DANE²⁴ en sus continuos estudios y encuestas como el censo poblacional o la encuesta nacional de hogares realiza *site surveys* previos muy rigurosos. También se realizan *site surveys* utilizando imágenes de satélite para la investigación de fauna especialmente de especies en estado silvestre para determinar sus costumbres como migración, reproducción y comportamiento social. Cada estudio *site survey* tiene su metodología propia dependiendo del área de aplicación.

En WLANs es muy importante para determinar los efectos de las ondas de radio propagadas. El objetivo principal del *Site Survey* es suministrar la suficiente información para determinar la ubicación y el número de APs que se deben instalar para proporcionar la cobertura adecuada. También detecta la presencia de fuentes de interferencias y la existencia de otras redes inalámbricas que podrían degradar el funcionamiento de la red. Gran parte del diseño de una WLAN es identificar la ubicación de los APs para proveer una interfase con los recursos de la red cableada y una adecuada cobertura para los usuarios móviles.

Si una WLAN fuese instalada en un área completamente abierta, libre de paredes, muros de concreto y muebles, las ondas de radio de los dispositivos inalámbricos serían capaces de mantener un patrón de radiación omnidireccional, haciendo más fácil la predicción del máximo rango de operación de todos los dispositivos y la ubicación de los APs. La construcción de una edificación ofrece ondas de radio a través de los diferentes pisos, por ejemplo, depende del método utilizado entre pisos. El rango es más grande si las ondas pasan a través de drywall, es menor si pasa a través de concreto y es muy pobre si pasa a través de metal.

La siguiente tabla muestra la interferencia de ondas las RF frente a diferentes materiales:

²⁴ Departamento Administrativo Nacional de Estadísticas.

Material	Ejemplo	Interferencia
Madera	Techos / Machimbres	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes	Baja
Ladrillo	Paredes	Media
Hojas	Árboles	Media
Cuerpo Humano	Muchedumbre	Media
Agua	Lluvia / Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio (con mucho plomo)	Ventanas	Alta
Metal	Vigas	Muy alta

Tabla E.1. Interferencia de las ondas RF

Cintas o láminas de metal en vidrios, paredes reforzadas con acero, pisos en cemento, paredes con aislamientos, escaleras de emergencia y elevadores son ejemplos típicos donde se reducirá el rango de la señal.

El único método verdadero para un óptimo desempeño de la WLAN es probar empíricamente la correcta ubicación de los APs y de los tipos de dispositivos que se utilicen como tarjetas NIC y antenas. No hay manera de determinar la distancia que una señal viajará sin un *site survey*.

La primera tarea es conseguir un plano de construcción o una maqueta a escala del lugar en el cual se quiere diseñar e instalar la red inalámbrica. Luego, sobre el plano o maqueta, se realiza un estudio, para definir la ubicación y cantidad de AP necesarios para cubrir el área deseada dentro de la red WLAN. Para esto se usan las denominadas *Site Surveys Tools*, herramientas que ayudan a comprobar el alcance y calidad de los enlaces inalámbricos. Dentro de estas herramientas están el software incorporado en las tarjetas NIC inalámbricas y un analizador de espectro.

Para un desarrollo exitoso del *Site Survey* se considera la siguiente metodología:

1. Adquirir un plano o maqueta del lugar.

Obtener un plano es un elemento esencial para continuar con los siguientes pasos del proceso.

2. Inspección visual

Inspeccionar y evaluar en forma visual el sector que se desea cubrir con la WLAN, para determinar la existencia de obstáculos que no aparezcan en el plano e identificar posibles fuentes de atenuación e interferencias de radiofrecuencias. En esta etapa se debe considerar si existen elementos y/o características del lugar que degraden el funcionamiento de la red WLAN.

3. Identificación del área de cobertura.

Identificar en el plano, las áreas que se desea abarcar con la WLAN.

4. Ubicación preliminar de los AP.

Definir la ubicación de los AP en forma preliminar, considerando la potencia de transmisión, tipo de antena y disponibilidad de red eléctrica, red de datos y el alcance del AP. La ubicación de los AP necesarios para dar cobertura al área deseada, depende del alcance de cada uno de estos. Según Wi-Fi, los APs logran un alcance nominal en interiores (Indoor) de 100m y en exteriores (Outdoor) de 400m.

Otro análisis que se puede realizar es la atenuación que experimenta la potencia de la señal a medida que se propaga.

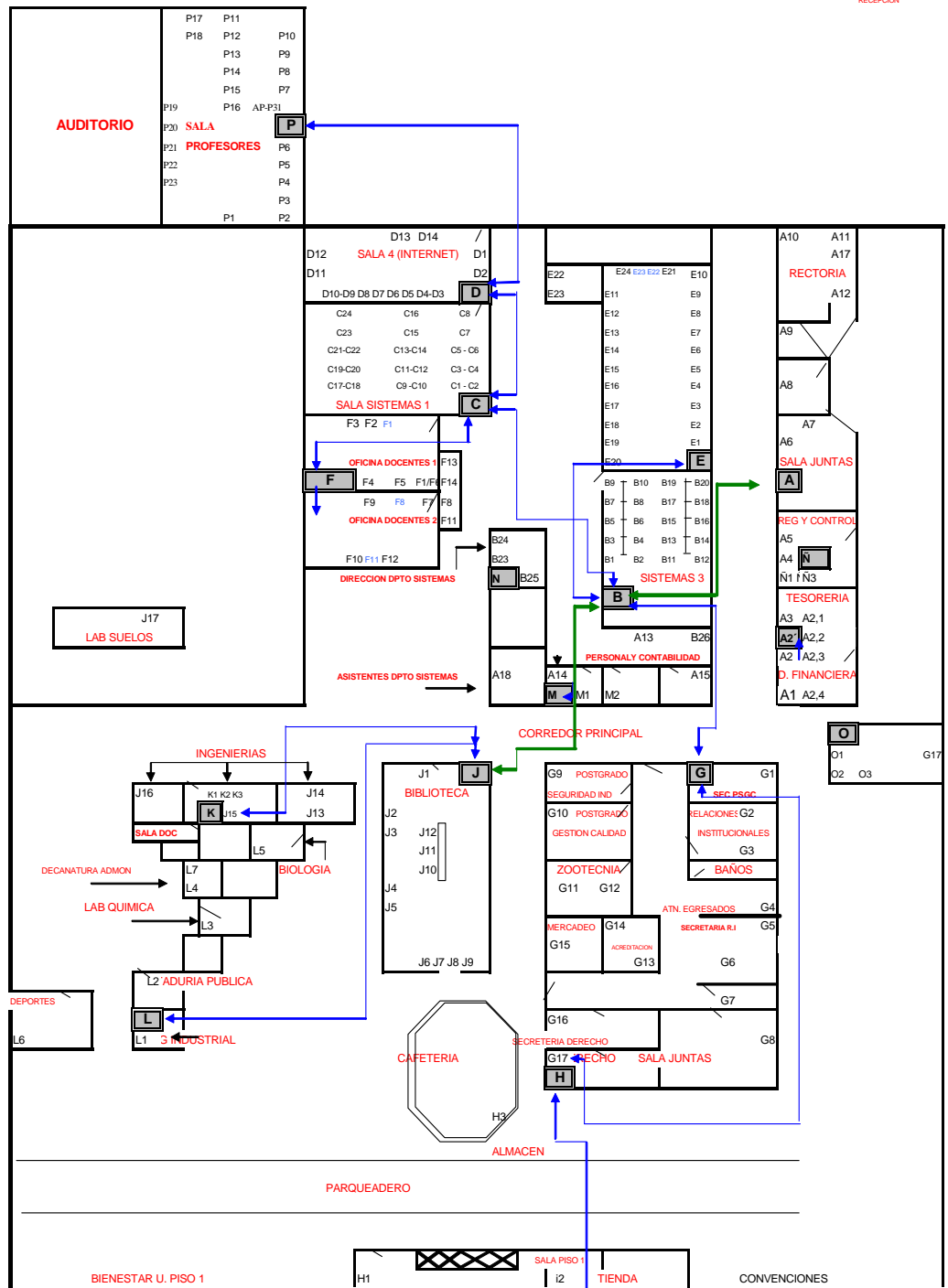
5. Verificando la ubicación de los AP.

Verificar la ubicación de los AP. Para corroborar si la ubicación preliminar es correcta se utilizan las *Site Surveys Tools*. Para realizar las pruebas de cobertura no es necesario tener conexión con la red cableada, ya que se realiza enviando pequeños paquetes de datos al AP, desde la STA, a través del comando *ping* en DOS. Un computador ejecutará continuamente el comando *ping* y se consignarán las estadísticas como tiempo mínimo, máximo, promedio, del recorrido ida y vuelta de los datos, así como el porcentaje de paquetes perdidos o tiempo de no respuesta.

6. Documentación

Una vez ubicados los AP, documente la información en forma adecuada, identificando los requerimientos del tipo eléctrico y de datos. En el plano indique la ubicación exacta de los dispositivos. Documentar la topología física y lógica de la red, modo de operación y rendimiento, de manera que esta documentación sirva como referencia de la nueva red instalada y de sus capacidades de funcionamiento. Cuando se prueba la red nuevamente, estos datos se comparan con los de la referencia, esto ayuda a resolver problemas específicos en la red causados por el ambiente, poco mantenimiento, entre otros.

ANEXO F. PLANO ESQUEMÁTICO RED LÓGICA UNIAGRARIA



Fuente: PRESING LTDA

ANEXO G. ALGUNAS HERRAMIENTAS SOFTWARE MONITOR WLANS

Herramienta	Sitio Web	Descripciones
NetStumbler	www.netstumbler.com	Identificador de APs, escucha los SSID y manda señales buscando APs
Kismet	www.kismetwireless.net	Sniffer y monitor de WLANs- de forma pasiva monitorea el trafico inalámbrico, ordena la información para identificar SSIDs, direcciones MAC, canales y velocidades de conexión.
Wellenreiter	http://packetstormsecurity.nl	Herramienta para descubrir WLANs- Usa la fuerza bruta para identificar APS de bajo tráfico, oculta su verdadera MAC y se integra con GPS.
THC-RUT	www.thehackerschoice.com	Herramienta para descubrir WLANs- Usa la fuerza bruta para identificar APS de bajo tráfico- Su primera herramienta en una red desconocida.
Ethereal	www.ethereal.com	Analiza WLANs- permite surfear de forma interactiva la información capturada, observando información detallada de todo el tráfico inalámbrico.
WepCrack	http://sourceforge.net/projects/wepcrack	Rompe la encriptación – Hace un crack de WEP utilizando las vulnerabilidades en la programación de RC4.
AirSnort	http://airsnort.shmoo.com	Rompe la encriptación- monitorea de forma pasiva las transmisiones, computando la llave de encriptación cuando se han capturado suficientes paquetes.
HostAP	http://hostap.epitest.fi	Convierte una estación WLAN para funcionar como un AP.

ANEXO H. ESPECIFICACIONES DISPOSITIVOS INALÁMBRICOS

TEW-430APB 54Mbps 802.11g Wireless Access Point TRENDNET



Especificaciones

Hardware

Standards:	IEEE 802.11g (Wireless LAN) IEEE 802.3u (Fast Ethernet)
Media Connector:	10/100Mbps, Half/Full Duplex
LED Indicators:	Power, LAN & WLAN
Power:	5V, 1.2A External Power Adapter
Dimensions:	124 x 86 x 40 mm (4.9 x 3.4 x 1.6 inches) (without antenna)
Weight:	124 x 86 x 40 mm (4.9 x 3.4 x 1.6 inches) (without antenna)
Temperature:	Operating: -0° ~ 40°C (32° ~104°F) Storage: -10° ~ 70°C (14° ~ 158°F)
Humidity:	Max. 90% (non-condensing)
Certifications:	CE, FCC
Wireless	
Frequency Range:	2.412 ~ 2.484 GHz
Modulation:	802.11b: DSSS 802.11g: DBPSK/DQPSK/CCK/OFDM
Protocol:	CSMA/CA with ACK
Data Rates (Auto Fallback):	802.11b: 11, 5.5, 2 and 1Mbps 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6Mbps

Operating Mode:	AP, WDS Bridge & Repeater
Channel:	AP, WDS Bridge & Repeater
Security:	64/128-bit WEP (Hex) & WPA 802.1x Authentication & MAC Address Access Control List (ACL)
Antenna:	1 x 2dBi Detachable Diversity Antennas with Female Reverse SMA Connector
Output Power:	13 dBm (min)
Transmit Power:	802.11b: 12dBm (typically) 802.11g: 15dBm (typically)
Receiving Sensitivity:	54Mbps: -68dBm @ 10% PER (Packet Error Rate) 11Mbps: -81dBm @ 8% PER (Packet Error Rate)

* Note: For optimal results in extending your wireless range with wireless antenna installations, we recommended that you consult a professional installer for site survey, safety precautions, and proper installation.

TEW-432BRP 54Mbps 802.11g Wireless Firewall Router



Especificaciones

Hardware

Standards

Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), ANSI/IEEE 802.3 Auto Negotiation

Wireless: IEEE 802.11b (11Mbps), IEEE 802.11g (54Mbps)

WAN

1 x 10/100Mbps Auto-MDIX Port (Internet)

LAN

4 x 10/100Mbps Auto-MDIX Port

Connection Type

Dynamic IP, Static (Fixed) IP, PPPoE, PPTP

Network

TCP/IP, NAT, PPPoE/PPTP, HTTP, DHCP Server/Client

Protocols

LED Indicator

Power, System, WLAN: ACT

WAN: Link, ACT & Speed; LAN: Link, ACT & Speed

Dimension (L x W x H)

147 x 115 x 35 mm (5.8 x 4.5 x 1.4 inches)

Dimension (L x W x H)

147 x 115 x 35 mm (5.8 x 4.5 x 1.4 inches)

Temperatura

226g.(8 oz.)

Humidity

Max. 95% (Non-Condensing)

Power Adapter

5V DC, 2.5A External Power Adapter

Certification

FCC & CE

Wireless

Frequency

2.412 to 2.484GHz (Industrial Scientific Medical Band)

Module Technique

802.11b: CCK (11 and 5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps)

802.11g: OFDM

Antenna

1 x 2dBi External Detachable Dipole Antenna (Female Reverse SMA Connector)

Media Access Protocol

CSMA/CA with ACK

Security

64/128-bit WEP, 802.1X/ WPA, WPA-PSK, MAC Address Filter, Protocol Filter

Transmit Power

13 dBm (typically)

Data Rate

802.11b: 11Mbps, 5.5Mbps, 2Mbps, and 1Mbps

802.11g: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps and 6Mbps

Receiving Sensitivity

11Mbps 8% PER @ -85 dBm (typical)

54Mbps 10% PER @ -70 dBm (typical)

Channels

11 Channels (US), 13 Channels (EU)

TEW-401PC 54Mbps 802.11g Wireless PC Card



Especificaciones

Hardware

Adapter Type:	32-bit CardBus PCMCIA Type II (fits PCMCIA Type II or Type III slot)
Standards:	IEEE 802.11g draft and IEEE 802.11b
Driver Supports:	Windows 98SE/ME/2000/XP
Data Rate (auto fallback):	802.11b: 11Mbps, 5.5Mbps, 2Mbps, and 1Mbps 802.11g: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps and 6Mbps
Module Technique:	802.11b: CCK (11 and 5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps) 802.11g: OFDM
Antenna:	Build-in Diversity Patch Antenna
Media Access Protocol:	CSMA/CA with ACK
Frequency:	2.4 to 2.497GHz (Industrial Scientific Medical Band)
Output Power:	15dBm (max.)
Receiving Sensitivity:	11Mbps 10 – 5 BER @ -80 dBm (typical) 54Mbps 10 – 5 BER @ -65 dBm (typical) -65 dBm – 54 Mbps, -67 dBm – 48 Mbps, -70 dBm – 36 Mbps, -75 dBm – 24 Mbps, -78 dBm – 18 Mbps, -82 dBm – 12 Mbps, -85 dBm – 9 Mbps, -89 dBm – 6 Mbps.
Power Consumption:	Operating: 3.3VDC (TX: 550mA, RX: 350mA). Idle: 3.3VDC, 225mA
Radio Disabled:	3.3VDC <10mA
Channels:	11 Channels (US/Canada), 13 Channels (EU)
Dimensions (L x W x H):	118 x 54 x 8.5 mm (4.65 x 2.1 x 0.33 inches)
Weight:	42.5g. (1.5 oz.)
Operating Temperature:	0° ~ 50° C (32° ~ 122° F)
Storage Temperature:	-20° ~ 65° C (-4° ~ 149° F)
Humidity:	Max. 95% (Non-condensing)
Certification:	FCC, CE

* Note: For optimal results in extending your wireless range with wireless antenna installations, we recommended that you consult a professional installer for site survey, safety precautions, and proper installation.

TEW-AO080 8dBi Outdoor Omni-Directional Antenna



Especificaciones

Hardware

Frequency Range

2400 ~ 2500MHz

Gain

8dBi

VSWR

2.0:1 Max

Polarization

Linear, vertical

HPBW/ Horizontal

360°

HPBW/ Vertical

15°

Power handling

50W (cw)

Down tilt

0°

Impedance

50 Ohms

Connector

N-Type Female

Survivalwind speed

216 km/h

Lightning protection

DC ground

Certification

CE, FCC

Dimension

25 x 80 x 520mm (0.98 x 3.15 x 20.47 in.)

Weight

323 g (11.4oz.)

Temperatura

-40°C ~ 80°C (-40°F ~ 176°F)

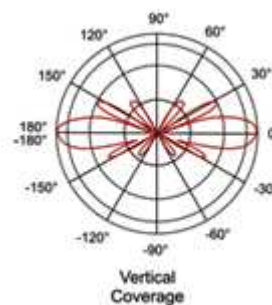
Humidity

100% at 25°C (77°F)

Certification

100% at 25°C (77°F)

Patrones de Radiación



- Note: For optimal results in extending your wireless range with wireless antenna installations, we recommended that you consult a professional installer for site survey, safety precautions, and proper installation.

WRT54G Wireless-G Broadband Router



Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE draft 802.11g
Channels	11 Channels (USA, Canada) 13 Channels (Europe) 14 Channels (Japan)
Ports	Internet One 10/100 RJ-45 Port for Cable/DSL Modem LAN Four 10/100 RJ-45 Switched Ports One Power Port
Cabling Type	Category 5 Ethernet Network Cabling or better
Data Rate	Up to 54Mbps (Wireless), 10/100Mbps (Ethernet)
LEDs	Power, DMZ, Diag WLAN Act, Link LAN Link/Act, Full/Col, 100 Internet Link/Act, Full/Col, 100
Transmit Power	15 dBm
Modulation	802.11b CCK, DQPSK, DBPSK draft 802.11g OFDM
Network Protocols	TCP/IP, IPX/SPX, NetBEUI
Environmental	
Dimensions	7.32" x 6.89" x 1.89" (186 mm x 175 mm x 48 mm)
Unit Weight	17 oz. (0.482 kg)
Certifications	FCC Class B
Operating Temp.	32°F to 104°F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing

ANEXO I. PRESING LTDA



Proyectos Especiales de Ingeniería, PRESING LTDA es una empresa de profesionales en las áreas de ingeniería eléctrica, electrónica y telecomunicaciones, con comprobada experiencia de más de 18 años en la ejecución de obras eléctricas y de cableado estructurado; suministro, montaje y mantenimiento de equipos de soporte eléctrico como reguladores de voltaje, sistemas ininterrumpidos de potencia UPS y equipos de telecomunicaciones.

Cuenta con verdaderos profesionales en Redes de Cableado Estructurado y Eléctrico, Regulación de Voltaje, Seguridad, Vigilancia y Control suministrando e instalando los mejores productos del mercado.

Presing Ltda. se encuentra en el proceso de cambio y constante actualización en tecnologías inalámbricas, diseño, implementación y puesta en marcha de proyectos de esta índole; ofreciendo así una mayor demanda de Ingenieros Electrónicos o afines.

Con su permanencia en el mercado por más de 18 años Presing Ltda. ha brindado a su clientela la solución más completa a sus necesidades en lo relacionado con Redes Lógicas y Eléctricas en Centros de Cómputo, Edificios Inteligentes y Áreas Industriales. Se ha preocupado por atender sectores como Agencias de Publicidad, Empresas Integradoras de Sistemas, Industrias Metalmecánica, Petroleras, Oficinas de profesionales en las diversas áreas, Sector Salud, Sector educativo, etc. y en general todos aquellos establecimientos donde se procesan datos y se usan las telecomunicaciones.

Presing Ltda. se ha preocupado de manera especial en representar las marcas de productos de la más alta calidad y mantenerlas disponibles en bodega con el fin de brindar suministro constante tanto de equipos nuevos como de equipos para demostración y soporte. De la misma forma estamos capacitando permanentemente a nuestro personal técnico y profesional para estar siempre a la vanguardia y así asesorar a nuestros usuarios al momento de ofrecer una solución definitiva. Al ofrecer tecnología de punta les aseguramos que los productos que nuestra empresa distribuye e instala estarán vigentes por muy largo tiempo antes de ser cubiertos por la obsolescencia. Así mismo tenemos a disposición una amplia gama no solo de marcas sino también de precios los cuales adaptamos al presupuesto de cada cliente.

La calidad de nuestros productos hace la clase de clientes que hoy tenemos y son una razón para seguir mejorando cada día.

Presing es distribuidor de:

Equipos de protección eléctrica y baterías para UPSs

UPS y reguladores *Apc - Tripp Lite – Powerware – Cdp – Atse*

Csb - Rocket - Coexito - Exide - Yuasa – Dynasty

Equipo activo para redes:

Hubs, switches, routers, modems *3com - Cisco – TrendNet – Netgear
Qpcom*



Línea de productos para redes LAN basados en tecnología Ethernet, Giga ethernet, fibra o Wireless (inalámbrico). Así como servidores de impresión, Internet, y todos los accesorios para el mayor rendimiento de su red.

Equipo para conectividad:



Cables UTP, STP, fibra óptica *Belden - Bertek - Amp - Condumex.*
Tomas categoría 5e, 6 y 7 *Siemon - Amp - Systimax - Quest – Panduit*

Equipo wireless desde 11mbps hasta 54mbps
Access Point, tarjetas PCI/ PCMCIA *3com - TrendNet - Zoom - Avaya*



Equipos y accesorios para telefonía:

Plantas telefónicas, teléfonos, Acces. *Panasonic – Avaya*



- ☑ **Equipos de seguridad y vigilancia y control por Internet:**
Cámaras Web, IP y CCTV *Panasonic - Orinoco – TrendNet*



PRESING LTDA Tiene a su disposición Sistemas y Equipos, Cámaras para circuito cerrado de TV en todas sus versiones dependiendo de las necesidades del cliente. También se cuenta con todos los accesorios y mantenimiento preventivo y correctivo. Especialistas en sistemas de seguridad con cámaras CCTV²⁵ y cámaras para vigilancia IP, controlada mediante procesadores. Ofrece también la capacidad de integrar nuestras cámaras inalámbricas en Red a los sistemas cableados de CCTV tradicionales.

²⁵ CCTV: Circuito Cerrado de Televisión.