PROYECTO DE REDES INALÁMBRICAS DE AREA LOCAL - WLAN

K-TRONIX

DIEGO CLARO
NUBIA PIÑEROS
JUAN CAMILO USECHE

CORPORACION UNIVERSITARIA UNITEC

ESCUELA DE INGENIERIA

PROGRAMA DE TECNOLOGIA EN SISTEMAS

BOGOTA D.C. IIPL 2004

PROYECTO DE REDES INALÁMBRICAS DE AREA LOCAL - WLAN

K-TRONIX

DIEGO CLARO
NUBIA PIÑEROS
JUAN CAMILO USECHE

Trabajo para optar al título de
Tecnólogo en sistemas

Director
OSCAR CUÉLLAR
Licenciado en Electrónica

CORPORACION UNIVERSITARIA UNITEC

ESCUELA DE INGENIERIA

PROGRAMA DE TECNOLOGIA EN SISTEMAS

BOGOTA D.C. IIPL 2004

NOTA DE ACEPTACION

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogota, Septiembre 15 de 2004

AGRADECIMIENTOS

Agradecemos la valiosa orientación del Licenciado Electrónico Oscar Cuéllar y a cada una de las personas que nos colaboraron en el desarrollo de este proyecto; a Sergio Moreno de K-TRONIX que nos apoyo en el proceso y a todos los Docentes a lo largo de nuestra carrera..

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

AAA: (*Authentication, Authorization and Accounting*) marco que define los elementos básicos para la autentificación de usuarios, el manejo de peticiones de autorización y la realización de la contabilidad del sistema.

AES: (*Advanced Encryption Standard*) Estándar de Encriptación Avanzada, potente método de encriptación para datos privados en el protocolo de seguridad IEEE 802.11i (WPA2).

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

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

CRC (Cyclic Redound Check) Chequeo Redundante Cíclico, método de cálculo de bits de paridad que se utiliza para la detección de errores en las redes de datos por paquetes.

DFS (Dynamic Frequency Selection) Selección Dinamica de Frecuencia.

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

EAP (Extensible Authentication Protocol) Protocolo de Autentificación Extensible, extensión del protocolo PPP que proporciona un mecanismo estándar para aceptar métodos de autentificación adicionales.

EAPOL (EAP over LAN) Nombre genérico equivalente a la norma IEEE 802.1x dado que consiste en el envío de mensajes EAP sobre redes LAN ya sean cableadas o inalámbricas, incluyendo además las Token-Ring y FDDI.

ESS (Extended Service Set) Grupo de Servicio Extendido, formado por la unión de dos o más BSS.

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

FCC (Federal Communications Commission) Comisión Federal de Comunicaciones, encargada de las regulaciones en el ámbito de las comunicaciones en Estados Unidos y enmarcada en la asignación y uso del espectro electromagnético de este país.

FDDI (Fiber Distributed Data Interface) Red de área metropolitana que utiliza un anillo unidireccional de fibras ópticas a la velocidad de 100 Mb/s.

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

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

IAPP (Inter-Access Point Protocol) Protocolo de comunicacación entre puntos de acceso.

SIDD (Service Set Identifier) Identificador del Grupo de Servicio, seudónimo de red que identifica el perímetro de cobertura de uno o más puntos de accesos.

IBSS (Independient Basic Service Set) Grupo de Servicio Básico Independiente, conjunto de estaciones que se comunican entre sí en ausencia de un punto de acceso, característica típica de las redes ad hoc.

IEEE (Institute of Electrical and Electronics Engineers) Instituto de Ingenieros Eléctricos y Electrónicos.
IEEE 802 Comité de la IEEE organizado para crear los estándares de las Redes de Área Local. La IEEE 802.11 especifica lan normas para la redes LAN inalámbricas.

ICV (Integrity Check Value) Valor Íntegro de Chequeo.

ISM (Industrial Scientific Medical) Bandas del espectro electromagnético destinadas a las aplicaciones industriales, científicas y médicas. Comprenden los rangos de frecuencia 902-928 MHz, 2.4-2.4835 GHz y 5.725-5.85 GHz.

IV (Initialization Vector) Vector de Inicialización.

LAN (Local Area Network) Red de Área Local.

MAC (Medium Access Control) Subnivel de Control de Acceso al Medio dentro del nivel de enlace en una red LAN.

MIC (Message Integrity Checker) Verificador de Integridad de Mensaje.

NIC (Network Interface Card) Tarjeta de Interfaz de Red, dispositivo equipado con una antena para la comunicación inalámbrica en una PC.

OFDM (Orthogonal Frequency Division Multiplexing) Multiplexación por División de Frecuencia con portadoras Ortogonles.

PPP (Point-to-Point Protocol) Protocolo Punto a Punto.

PRNG(Pseudo Random Number Generator) Generador de Números Pseudo-aleatorios.

QoS (Quality os Service) Calidad de Servicio, concepto que permite asegurar determinadas prestaciones al usuario.

RADIUS (Remote Authentication Dial-In User Service) Servicio de Usuario de Autentificación Remota.

TKIP (Temporal Key Integrity Protocol) Protocolo de Integralidad de Clave Temporal.

TPC (Transmition Power Control) Control de Potencia de Transmisión.

WECA (Wireless Ethernet Compatibility Alliance) Alianza de Compatibilidad en Ethernet Inalámbrica, asociación internacional encargada de certificar la interoperatividad de las redes LAN inalámbrica. Es además reconocida por el alias Wi-Fi, marca o certificación de aquellos productos acogidos a esta normativa.

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

Wi-Fi (ver WECA).

Wi-Fi5 Certificación Wi-Fi para la tecnología dentro de la banda de los 5 Ghz.

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

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

Referencias

[1] Stalling, Williams, Local & Metropolitan Area Networks, pp. 374, 377-79.

[2] Kumar, Vinod; Carrez, François; Riganati, John (2001). "Principales Tecnologías Para Redes Radio Ad Hoc". **Revista de Telecomunicaciones de ALCATEL** (3): 207-209.

[3] Harris, Shon (2001). "802.11 Security Shortcomings". **Windows 2000 Magazine** 7(16): 47-51.

[4] Erlanger, Leon (2003), "Real Security for Wireless LANs". **PC Magazine**. 22(13): 72.

INTRODUCCION

Dentro del enorme horizonte de las comunicaciones inalámbricas y la computación móvil, las redes inalámbricas van ganando adeptos como una tecnología madura y robusta que permite resolver varios de los inconvenientes del uso del cable como medio físico de enlace en las comunicaciones, muchas de ellas de vital importancia en el trabajo cotidiano. Una vez que se ha tenido la oportunidad de haber hecho uso de algún dispositivo inalámbrico que proporcionase datos o información requerida con independencia del lugar, es prácticamente imposible olvidar las características que los hacen tan especiales. Los equipos inalámbricos otorgan la libertad necesaria para trabajar prácticamente desde cualquier punto del planeta e, incluso, permiten el acceso a todo tipo de información cuando se está de viaje. No importa que el sistema inalámbrico esté accediendo al correo electrónico desde un aeropuerto o recibiendo instrucciones desde el despacho para realizar alguna tarea, lo realmente relevante de esta tecnología es la extremada efectividad que se logra al poder mantener una conexión de datos con una red desde cualquier sitio remoto del planeta. Por otra parte, las comunicaciones de radio han estado a nuestra disposición desde hace ya bastante tiempo, teniendo como principal aplicación la comunicación mediante el uso de la voz. Hoy en día, millones de personas utilizan los sistemas de radio de

dos vías para comunicaciones de voz punto a punto o multipunto. Sin embargo, aunque los ingenieros ya conocían las técnicas para modular una señal de radio con la cual conseguir el envío de datos binarios, sólo recientemente han podido desarrollar y desplegar servicios de datos a gran escala.

Como muestra del complejo campo de las redes sin cables, el mundo de los denominados datos inalámbricos incluyen enlaces fijos de microondas, redes LAN inalámbricas, datos sobre redes celulares, redes WAN inalámbricas, enlaces mediante satélites, redes de transmisión digital, redes con paginación de una y dos vías, rayos infrarrojos difusos, comunicaciones basadas en láser, Sistema de Posicionamiento Global (GPS) y mucho más. Como se puede ver, una variada y extensa gama de tecnologías, muchas de las cuales son utilizadas con suma profusión por millones de usuarios en el transcurrir del día a día, sin saber cómo ni por qué la información ha llegado hasta ellos. Tampoco hay que olvidar los numerosos beneficios que aporta el uso de los dispositivos inalámbricos, ya que gracias a ellos se logran realizar conexiones imposibles para otro tipo de medio, conexiones a un menor costo en muchos escenarios, conexiones más rápidas, redes que son más fáciles y rápidas de instalar y conexiones de datos para usuarios móviles. Como vemos, el panorama de las redes inalámbricas es casi tan extenso o más que el de las propias redes convencionales, a las que estamos más habituados. Debido a la impresionante variedad de tecnologías, configuraciones, dispositivos, topologías y medios, relacionados con las redes inalámbricas debemos limitar la profundidad y extensión de este documento centrándonos en

las redes inalámbricas de área local. Este tipo de redes, por la proximidad al mundo de la pequeña y mediana empresa, las hace, ya no sólo mucho más accequibles, sino que su posible implantación en cualquier empresa o entorno de trabajo en grupo sea una realidad totalmente tangible con la mera inversión de dichos medios, sin que los costes de adquisición sean la barrera que impida el despegue definitivo de las redes inalámbricas. En síntesis, las redes LAN sin cables o más conocidas por el sobrenombre de WLAN (Wireless Local Area Network) no son algo realmente novedoso ni revolucionario dentro del mundo de la informática. Desde hace unos cuantos años, el atractivo de esta clase de redes hizo que aparecieran los primeros sistemas que utilizaban ondas de radio para interconectar computadores.

OBJETIVOS

GENERAL

Elaborar una propuesta para el diseño de una Red WLAN de acuerdo a las normas establecidas en la actualidad, teniendo en cuenta las necesidades de la empresa y sugiriendo los requerimientos funcionales de acuerdo a la relación costo-beneficio.

ESPECÍFICOS

- Evaluar la Red Lan Existente en el Punto de Venta de K-tronix Calle 94 para determinar los componentes necesarios para la implementación de una Red Inalámbrica.

- Conocer los requerimientos de las aplicaciones de la empresa y la capacidad de los enlaces en el punto de trabajo

- Determinar el numero de equipos instalados y su configuración para habilitarlos en la WLAN

- Establecer un nivel de seguridad para la Nueva WLAN de manera que personas no autorizadas puedan utilizarla.

FORMULACIÓN DEL PROBLEMA

De acuerdo a las visitas realizadas a la empresa K-TRONIX sede calle 94 y con la información obtenida por parte de la misma, se analizaron las necesidades actuales de este punto de venta a saber:

1. Acceder a información compartida en dicho punto de venta y poder visualizar datos existentes de un equipo a otro, aprovechando las capacidades de comunicación inalámbrica con que cuentan algunos equipos del almacén y los que están a la venta,
2. Comunicación entre empleados a través de Laptops, PDAs, etc...
3. Obtener información veraz de los productos y ventas a cualquier momento y en cualquier lugar de la zona de ventas a través de un equipo habilitado para comunicación Inalámbrica.
4. Aplicar la Tecnología de comunicación inalámbrica inicialmente al Punto de Venta de KTRONIX Calle 94, sin incluir la parte administrativa.
5. Demostración de equipos inalámbricos a los clientes

La implementación de redes inalámbricas para conectar sucursales y generar conectividad sin cables en los espacios de trabajo es una excelente alternativa

para las empresas. En caso de conectar sucursales suele ser un ahorro en conectividad a corto plazo. Generar HOT SPOTS (Áreas de Conexión Inalámbrica) dentro de la organización permite mayor movilidad para estar conectado a los sistemas internos o a Internet.

Actualmente no se cuenta con una red inalámbrica dentro del área comercial, por lo cual es imposible aprovechar todas las capacidades de conexión de los nuevos PDA, Laptop's limitando así la posibilidad del cliente de ver en funcionamiento una WLAN con diferentes dispositivos de ultima generación ofrecidos en este almacén.

Teniendo en cuenta las necesidades mencionadas anteriormente se formula el siguiente problema:

¿Con la instalación de una red inalámbrica, clientes, personal de administración y servicios de K-tronix pueden navegar por Internet, mandar o recibir correos electrónicos, y participar en los cursos 'online' y capacitaciones que oferta la empresa, entre otras muchas actividades, sin necesidad de conectarse a ningún cable gracias a la estandarización de la tecnología Wi-Fi de redes inalámbricas?

JUSTIFICACION

En la actualidad la zona de ventas de K-TRONIX de la calle 94 no cuenta con un sistema de red que le permita comunicarse a nivel interno, solo utilizan diskettes y comunicación vía internet para el envío de información. Adicionalmente en este punto el cliente no tiene acceso a la diversidad de productos que ofrece K-TRONIX, es necesario la instalación de la red para que el usuario se pueda informar de la existencia de productos de K-TRONIX a nivel nacional.

Con la implementación de este nuevo sistema en redes, que permita acceder a información compartida, tomando en cuenta las pautas que actualmente utiliza este punto de venta y las nuevas sugerencias que podemos aportar a ella, sus labores serán más eficientes y precisas para ofrecer una buena y oportuna calidad al cliente.

1. ANTECEDENTES DE LA EMPRESA

Alkosto con el fin de seguir prestando el mejor servicio a sus clientes creó en el año 2000, K-Tronix, una tienda especializada en las líneas de electrónica, electrodomésticos e informática, con un amplio surtido de productos, las marcas mas reconocidas nacional e internacionalmente y la mejor oferta de productos de alta tecnología.

K-tronix con el respaldo y la experiencia de ALKOSTO ofrece a sus clientes un servicio personalizado, que se logra mediante la capacitación continua de todo el personal. Al mismo tiempo el equipo de compras, trabaja por tener productos de ultima tecnología y accesorios para cumplir con la fuerte demanda.

1.1 RESEÑA HISTÓRICA

Alkosto, es la primera HIPERBODEGA colombiana, creada en 1988 como una respuesta moderna a la distribución. Atiende a "grandes consumidores" (tenderos, instituciones, empresas, hoteles, restaurantes y hogares de grandes consumos), ofreciendo una variedad de artículos que van desde ferretería, llantas,

construcción hasta granos; caracterizados por empaques que generan grandes ahorros, denominándose así productos inteligentes.

Es una empresa de capital 100% colombiano, conformada por 3 áreas de negocios, autónomas en su gestión comercial (ventas al detal, distribución y textiles), pero agrupadas bajo una misma junta directiva. La organización tiene aprox. 950 empleados.

La compañía está especializada en comercializar productos de consumo masivo, haciéndolos llegar a los principales canales de comercio, prestando excelentes servicios de venta a sus Clientes y proporcionando satisfacción a sus Proveedores por la distribución de sus productos e investigar los métodos para lograr la mayor eficiencia en distribución; y en interrelacionar todos los procesos para alcanzar la Excelencia en el Servicio.

En el negocio de distribución de productos de consumo masivo, cuenta con cobertura en el 75% del país, abarcando las regiones de Cundinamarca, Boyacá, Santanderes, Territorios Nacionales, Cauca, Valle, Nariño, Putumayo, Tolima, Huila, Caquetá, Casanare, Meta, Boyacá, Caldas, Chocó, Cesar, Magdalena.

Alkosto con el fin de seguir prestando el mejor servicio a sus clientes creo en el año 2000, K-Tronix, una tienda especializada en las líneas de electrónica, electrodomésticos e informática, con un amplio surtido de productos, las marcas

más reconocidas nacionales e internacionales y la mejor oferta de productos de alta tecnoiogía.

En estos cuatro años de vida, K- tronix se ha hecho de cuatro puntos de venta, ubicados en puntos estratégicos de la ciudad así:

- Calle 94 con carrera 15: Uno de los más importantes puntos de venta, dada su ubicación se ha consolidado en el sector, con una amplia zona de ventas, personal especializado, parqueadero vigilado, y excelentes precios.
- Calle 124 con Carrera 7: Atiende un gran mercado ubicado en el norte de la ciudad, tiene 2 pisos divididos en diferentes secciones de productos, con personal especializado para asistir al cliente en su compra.
- Centro Comercial Unicentro (2003): Reconocido como el centro comercial mas tradicional de Bogota y con mas de 25 años de existencia, K-tronix se anota un punto al consolidar un nombre en los elementos de la tecnología al lado de gigantes como Panamericana y Carsa.
- Centro Comercial Plaza de las Américas (2004): atiende a la población del occidente y sur de Bogota, ubicado en el agitado sector de Ciudad Kennedy.

En este sentido, K-tronix cuenta con seis líneas de productos a saber:

1. Línea informática: con la venta de computadores, laptops, ipods, cámaras digitales Agendas electrónicas de última generación.
2. Línea car audio: radios para carro, amplificadores, subwoofer de las marcas más reconocidas, también prestan el servicio de instalación profesional.
3. Línea entretenimiento: DVD, televisores de plasma, pantallas gigantes, televisores, consolas de video juegos.
4. Línea electrodomésticos: Lavadoras, Secadoras Neveras.
5. línea audio: Parlantes, Home teathers, equipos de sonido.
6. línea de video: cámaras filmadoras y digitales, tarjetas de memoria.

Empresas como Samsung, Sony, Harman Kardon, Bose, Whirlpool, Palm, Alpine, Pioneer, Microsoft, Nintendo, etc. han confiado en K-tronix la distribución y venta de sus productos, con el fin de que el consumidor pueda acceder a ellos de manera fácil. Asimismo, K-tronix cuenta con contactos en los centros de servicios y reparación de las anteriores marcas, lo que posiciona a la empresa como líder en el mercado de la venta de productos de tecnología en Bogota, brindando al cliente una atención personalizada que va desde la introducción al producto hasta proporcionar servicio preventivo y correctivo al mismo.

K-tronix con el respaldo y la experiencia de ALKOSTO ofrece a sus clientes un servicio personalizado, que se logra mediante la capacitación continua de todo el personal. Al mismo tiempo el equipo de compras, trabaja por tener productos de ultima tecnología y accesorios para cumplir con la fuerte demanda.

2. DESCRIPCIÓN GENERAL DE LAS REDES LAN INALÁMBRICAS

Las redes LAN inalámbricas de alta velocidad ofrecen las ventajas de la conectividad de red sin las limitaciones que supone estar atado a una ubicación o por cables. Existen numerosos escenarios en los que este hecho puede ser de interés; entre ellos, se pueden citar los siguientes:

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

Y, por supuesto, el fenómeno asociado al término "inalámbrico", es decir, no tener que instalar más cables además de los de la red de telefonía y la red de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes domésticas y la experiencia de conexión desde el hogar.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles que cuentan con NIC inalámbricas. Esto permite al usuario desplazarse a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el usuario tendría que llevar consigo pesados cables y disponer de conexiones de red.

Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos podría estar disponible a través de zonas activas de redes inalámbricas públicas. Los aeropuertos, los restaurantes, las estaciones de tren y otras áreas comunes de las ciudades se pueden dotar del equipo necesario para ofrecer este servicio. Cuando un trabajador que está de viaje llega a su destino, quizás una reunión con un cliente en su oficina, se puede proporcionar acceso limitado al usuario a través de la red inalámbrica local. La red reconoce al usuario de la otra organización y crea una conexión que, a pesar de estar aislada de la red local de la empresa, proporciona acceso a Internet al visitante. En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 MB por segundo, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WAN inalámbricas estándar. Este ancho de banda es sin duda adecuado para que el usuario obtenga una gran

experiencia con varias aplicaciones o servicios a través de PC o dispositivos móviles. Además, los avances en curso de estos estándares inalámbricos continúa aumentando el ancho de banda, con velocidades de 54 MB.

2.1 ORGANIZACIONES Y ESTANDARES

El fundamento de muchas de las actuales redes inalámbricas se encuentra basado en el estándar IEEE 802.11, y más concretamente en las especificaciones IEEE 802.11b, IEEE 802.11a y IEEE 802.11g. Un consorcio, el "Wireless Ethernet Compatibility Alliance" (WECA), formado por un nutrido grupo de relevantes empresas, ha creado una nueva línea de productos de mayores prestaciones y de plena compatibilidad. Este consorcio ha establecido un estándar llamado Wi-Fi que permite la certificación de los productos acogidos a esta normativa para lograr que entre ellos existan una obligada interoperatividad y otros aspectos comunes de actuación como la facilidad de configuración, unanimidad de protocolos, modos de funcionamiento, así como las más elementales normas. Pero, independientemente del esperanzador futuro de las WLAN acogidas al Wi-Fi, dentro de este particular sector de las redes inalámbricas hay otras tecnologías que también aprovechan parte de la infraestructura de la cual hacen uso casi todos los dispositivos WLAN. En general, los sistemas LAN sin cables basados en el protocolo 802.11 hacen un exhaustivo uso de la banda de frecuencias de los 2,4 GHz. El porqué de este concreto rango de frecuencias puede resumirse en que en esta zona del espectro electromagnético no se requiere el uso de licencias tal y

como se lleva a cabo la regulación de los sistemas de radio, ya que en ellas se permite la transmisión de información en bandas del espectro, concretamente en las bandas llamadas ISM por su uso para aplicaciones industriales, científicas y médicas. Pero esta misma ventaja actúa a su vez de poderoso reclamo para otras tecnologías, sistemas o dispositivos inalámbricos que también basan su funcionamiento en esta área específica del espectro.

Las WLAN aunque son la base de la expansión y flexibilidad de muchas de las actuales redes LAN, pecan quizá de ser una solución más bien general y dirigida a entornos de trabajo en grupo y empresas que puedan sacar el máximo partido a sus capacidades. Precisamente, esta generalidad ha dado pie a que nuevas tecnologías como *Bluetooth* y *HomeRF*, surjan en torno al estándar 802.11, y aprovechando igualmente el rango de frecuencias de 2,4 GHz, han optado por especializarse en ofrecer una conectividad inalámbrica pero enfocada a unos usos mucho más particulares y en relación directa con los futuros hábitos de vida de los componentes de la moderna sociedad de principios del siglo XXI.

Bluetooth es una especificación para la industria informática y de las telecomunicaciones que describe un método de conectividad móvil universal con el cual se pueden interconectar dispositivos como teléfonos móviles, Asistentes Personales Digitales (PDA), ordenadores y muchos otros dispositivos, ya sea en el hogar, en la oficina o, incluso, en el automóvil, utilizando una conexión inalámbrica de corto alcance. Es un estándar que describe la manera en la que una enorme

variedad de dispositivos pueden conectarse entre sí, de una forma sencilla y sincronizada, con cualquier otro equipo que soporte dicha tecnología utilizando las ondas de radio como medio de transporte de la información. Técnicamente, la implementación de esta novedosa tecnología no entraña ninguna complicación técnica especialmente problemática ni sofisticada. Tampoco supone que los nuevos dispositivos equipados con esta tecnología deban sufrir profundas revisiones o modificaciones.

En sí, cada dispositivo deberá estar equipado con un pequeño chip que transmite y recibe información a una velocidad de 1 Mbps en la banda de frecuencias de 2,4 GHz que está disponible en todo el mundo, con ciertas particularidades según los diferentes países de aplicación, ya que es empleada con enorme profusión en numerosos dispositivos.

Con una finalidad muy similar, la tecnología *HomeRF*, basada en el protocolo de acceso compartido "Shared Wireless Access Protocol" (SWAP), encamina sus pasos hacia la conectividad sin cables dentro del hogar. Los principales valedores de estos sistemas, se agrupan en torno al Consorcio que lleva su mismo nombre HomeRF, teniendo a Proxim (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 producto 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 ("Bluetooth Special Interest Group"), el HomeRF Working Group (HRFWG) es un grupo de 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 Instituto de Estándares de Telecomunicaciones Europeo (ETSI) es otra de las reconocidas organizaciones de estandarización, responsable del desarrollo del estándar GSM para la telefonía celular digital. También son responsables de haber llevado a cabo durante los años 1991 y 1996 el proyecto HyperLAN, en el cual su objetivo primordial fue conseguir una tasa de transferencia mayor que la ofrecida por la especificación IEEE 802.11. 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 802.11.

Actualmente, el ETSI dispone de la especificación HyperLAN2 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 como el HyperLAN2 Global Forum (H2GF), con la intención de sacar al mercado productos basados en ese competitivo estándar.

2.1.1 Normalización IEEE

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

En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems). En 1993 también se constituye la IrDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de informática móvil (mobile computing) y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Por otra parte, WLANA (Wireless LAN Association) es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; 802.11b, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compatible con él, pero que proporciona aún mayores velocidades.

2.1.1.1 IEEE 802.11

Fue publicada el 1997, considerándose la primera norma de la familia IEEE 802.11, con operatividad dentro de la banda de los 2.4 GHz. Se lograron velocidades hasta 2 Mbps con una taza de datos de 1.2 Mbps. Emplea técnicas de modulación de espectro extendido por salto de frecuencia FHSS, o de secuencia directa DSSS.

Los sistemas LAN inalámbricos basados en el protocolo IEEE 802.11, explotan la banda de frecuencia correspondiente a los 2.4 GHz. El exhaustivo uso de esta zona del espectro electromagnético se debe a que no requiere de licencias para su explotación, libre de las restricciones de la regulación de los sistemas de radio. Estas bandas son destinadas a las aplicaciones industriales, científicas y médicas, nombradas ISM, a la que corresponden los rangos 902–928 MHz (banda 915 MHz), 2.4–2.4835 Ghz (banda 2.4 GHz), y 5.725–5.85 GHz (banda 5.8 GHz).

2.1.1.2 IEEE 802.11b

Se establece en 1999 como una evolución del estándar IEEE 802.11, operando en la misma banda, dentro de los 2.4 GHz. Este solo usa el espectro extendido de secuencia directa permitiéndole alcanzar velocidades hasta los 11 Mbps, similar a las conexiones de 10 Mbps de las Ethernet basadas en los grupos de trabajo, ahora con un mejor desempeño con respecto a su antecesor, aunque aún con una razón de datos pequeña que cae, aproximadamente, a la mitad de su velocidad total, de 5 a 6 Mbps como promedio.

La capacidad de la red no es uniforme y depende del entorno, las distancias y el número de usuarios conectados simultáneamente así como de las aplicaciones que se brinden y soliciten. En la práctica, un ancho de banda compartido y a esa razón de datos es suficiente para la mayor parte de las aplicaciones, excepto para flujos de video. Partiendo del elevado número de usuarios que hacen uso del servicio y que el ancho de banda es compartido entre estos, es posible instalar otros puntos de accesos en un mismo local con el objetivo de mejorar las prestaciones, aumentando el ancho de banda disponible. Haciendo uso de la norma IEEE 802.11b, la carga puede ser equilibrada con tres puntos de accesos instalados en el área, para un total de 33 Mbps y con mayor desempeño.

Si partimos de un análisis del ancho de banda, las redes WLAN, regidas por la norma IEEE 802.11b, requieren de 22 MHz mínimo, brindando la posibilidad de

operación de tres redes WLAN paralelas, dentro de la banda ISM con alrededor de 80 MHz (2.4–2.4835 Ghz).

Este estándar es uno de los más difundidos dentro de las normas inalámbricas dado que también explota las bandas ISM. Independientemente que aún su velocidad es menor que las alcanzadas por redes cableadas, sus capacidades en la prestación de servicios, cubre las necesidades de muchas organizaciones que solicitan esta tecnología, dadas sus ventajas sobre las cableadas en cuanto a movilidad.

Existe compatibilidad entre los productos IEEE 802.11b de diferentes proveedores, certificadas por la Alianza de Compatibilidad en Ethernet Inalámbrica WECA también llamada Wi-Fi Alliance, asociación internacional no lucrativa creada con el objetivo de certificar la interoperatividad de las redes LAN inalámbricas. Este consorcio, formado por un nutrido grupo de relevantes empresas, ha establecido el estándar Wi-Fi para la certificación de aquellos productos acogidos a estas normativas, obligándolos a una compatibilidad que va desde la facilidad de configuración hasta el modo de funcionamiento, entre otros aspectos comunes.

2.1.1.3 IEEE 802.11a

Este estándar fue ratificado en el año 1999, pero no es hasta diciembre del 2001 que se introduce en el mercado internacional, ahora con una velocidad hasta los 54 Mbps y frecuencias de trabajo en los 5 GHz, usando técnicas de multiplexación

por división de frecuencia sobre portadoras ortogonales OFDM empleando hasta 8 canales no solapados, equivalente a 8 puntos de acceso.

Al ser comparada con las normas IEEE 802.11 y 11b, notamos que brindan un mayor número de facilidades dado que soporta un elevado porcentaje de usuarios con una mayor razón de datos y menor probabilidad de interferencia con otras tecnologías dentro de su banda de trabajo.

Lamentablemente no existe compatibilidad, tanto inversa como directa, entre los productos (NIC y AP) regidos por las normas IEEE 802.11a y sus predecesores, dado que trabajan a diferentes frecuencias. No obstante, en la actualidad, los proveedores de dispositivos de redes inalámbricas, confeccionan equipos capaces de operar en las normas 11a y 11b de forma simultánea (Fig.1).

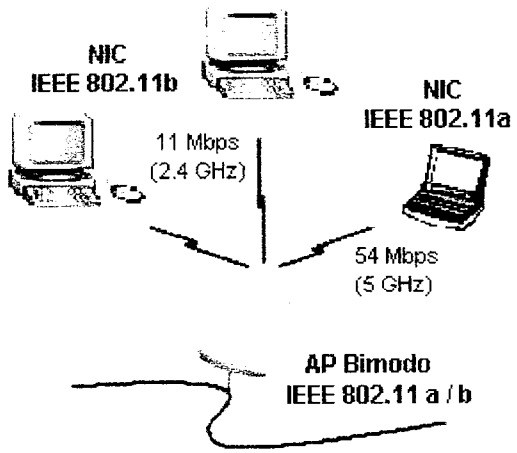


Figura 1. Desempeño de un Punto de Acceso bimodo.

En abril del 2002, *Cisco System Inc.* desarrolló la serie comercial *Cisco Aironet 1200 Series Access Point,* productos que acomodan ambas bandas del espectro radioeléctrico (2.4 y 5 GHz) dando como resultado 11 canales sin solapamiento, 8 desde la banda de los 5 GHz y otros 3 desde la de 2.4 GHz.

La Wi-Fi5 (Wi-Fi para la tecnología aplicable a la banda de 5 GHz) procede de la Wi-Fi original en la IEEE 802.11b. Esta organización se encarga de garantizar la interoperatividad entre equipos con igual fin, que exploten esta banda del espectro.

2.1.1.4 IEEE 802.11g

Este estándar fue aprobado en el 2001 y ya en octubre del siguiente año se da a conocer un preproyecto con disponibilidad de 54 Mbps de velocidad, dentro de la banda de los 2.4 GHz. Posibilita la interoperatividad con la norma IEEE 802.11b, limitándose a los 3 canales sin solapamiento con igual ancho de banda. Para lograr los 54 Mbps se usa la técnica OFDM similar a la norma IEEE 802.11a.

Existe compatibilidad ascendente con la tecnología DSSS, en cuyo caso, la velocidad se limita a los 11 Mbps. Esta interoperatividad implica que un cliente con un NIC normado según la IEEE 802.11b, puede desempeñarse dentro de un área de cobertura monitoreada por un AP IEEE 802.11g, y viceversa. Sólo se logran los

54 Mbps, cuando este intercambio de información, se establece entre dos productos normados dentro de este último estándar (Fig.2).

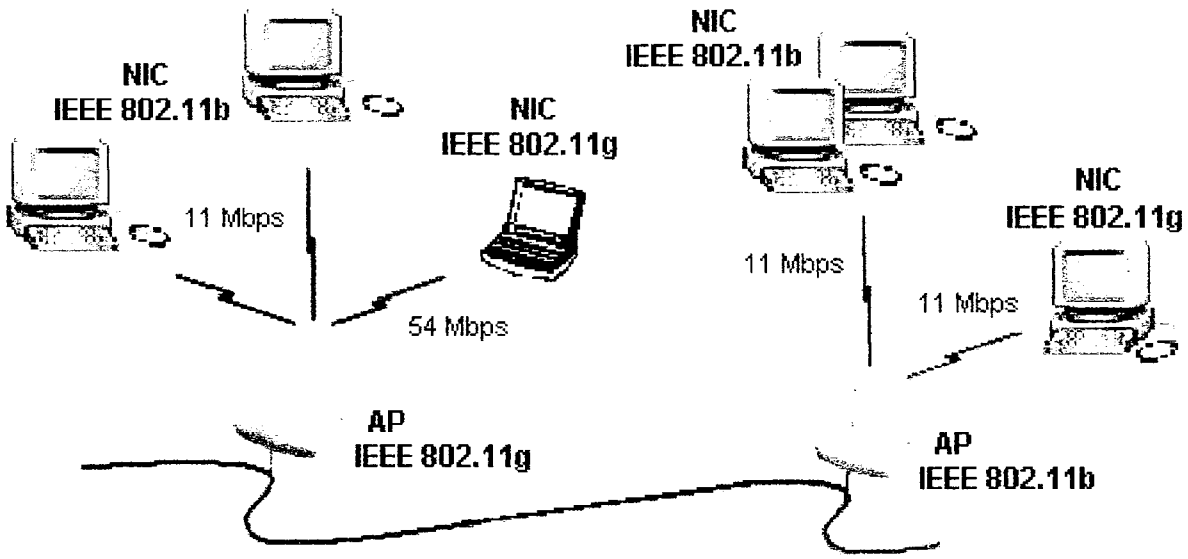


Figura 2. Interoperatividad entre los estándares IEEE 802.11b y 11g.

En noviembre del 2003, *3Com Corporation* introdujo al mercado una gama de soluciones inalámbricas con nuevos puntos de acceso y dispositivos (tarjetas y adaptadores) en tres modalidades para las redes LAN inalámbricas, logrando así, la combinación de seguridad avanzada con productos integrados que soportan los tres estándares Wi-Fi IEEE 802.11a, 11b y 11g.

2.1.2 Extensiones de los Estándares Inalámbricos

En adición a las normas anteriores y paralelamente con sus progresivas introducciones al mercado mundial, se fueron desarrollando otro conjunto de estándares destinados al perfeccionamiento de los servicios brindados por las redes de radio, ahora en términos de seguridad y calidad de servicio entre los de mayor importancia.

2.1.2.1 IEEE 802.11h

Esta norma responde a las exigencias europeas específicamente. Prevé la selección dinámica de frecuencia (DFS) y el control de la potencia de transmisión (TPC) para los equipos que operan en la banda de los 5 GHz, eliminando posibles interferencias en las comunicaciones satelitales, consideradas de carácter primario en este continente. Su desarrollo se favorece con el objetivo de competir con la norma europea HyperLAN, y de esta forma dominar terreno comercial dentro de las tecnologías inalámbricas.

2.1.2.2 IEEE 802.11d

Constituye un complemento al nivel de Control de Acceso al Medio (MAC) en la familia IEEE 802.11, proporcionando el uso, a escala mundial, de las redes WLAN de este estándar. Asegura que los puntos de acceso comuniquen la información

sobre los canales de radio admisibles, con niveles de potencia aceptables para los dispositivos de los usuarios.

2.1.2.3 IEEE 802.11e

Garantiza la adición del soporte QoS (calidad de servicio) al protocolo MAC. Posibilita la incorporación de aplicaciones de requerimientos especiales de tiempo como voz y video, así como videoconferencias sobre redes de radio normadas por la familia IEEE 802.11.

2.1.2.4 IEEE 802.11i

Incorpora la seguridad mediante la encriptación avanzada y procedimientos de autentificación, según los requerimientos de alta privacidad que sean solicitados. Es el equivalente a WPA2, última versión en seguridad de redes inalámbricas.

2.1.2.5 IEEE 802.11f

Especifica un protocolo entre puntos de acceso (IAPP del inglés Inter-access Point Protocol) para la comunicación entre estos, independientemente de los proveedores y la marca de los productos. Comprende la inscripción de un punto de acceso en una red y el cambio de información cuando un usuario se traslada

en la zona de cobertura gestionada por los puntos de acceso de diferentes orígenes.

La tabla 1 muestra un cuadro resumen de las nuevas especificaciones relacionadas con el IEEE 802.11:

Estándar	Espectro	Tasa Física Máxima	Tasa de Datos Nivel 3	Método de Transmisión	Compatibilidad
802.11	2.4 GHz	2 Mbps	1.2 Mbps	FHSS/DSSS	No
802.11a	5.0 GHz	54 Mbps	32 Mbps	OFDM	No
802.11b	2.4 GHz	11 Mbps	6-7 Mbps	DSSS	802.11
802.11g	2.4 GHz	54 Mbps	32 Mbps	OFDM	802.11/ 802.11b

Tabla 1. Estándares IEEE 802.11

2.2 TIPOS DE SISTEMAS DE ESPECTROS DISPERSOS

La tecnología de espectro ensanchado consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una portadora concreta lo que se hace es repartirla por toda la banda disponible. Este ancho de banda total se comparte con el resto

de usuarios que trabajan en la misma banda frecuencial. Existen tres tipos de tecnologías de espectro ensanchado:

- Espectro Ensanchado por Secuencia Directa (DSSS)
- Espectro Ensanchado por Salto en Frecuencia (FHSS)
- Espectro Ensanchado por Salto en Frecuencia (OFMD)

2.2.1 Tecnología de Espectro Ensanchado por Secuencia Directa (DSSS)

Esta técnica consiste en la generación de un patrón de bits redundante llamado *señal de chip* para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante mediante una portadora de RF. En recepción es necesario realizar el proceso inverso para obtener la señal de información original.

La secuencia de bits utilizada para modular cada uno de los bits de información es la llamada secuencia de Barker y tiene la siguiente forma:

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

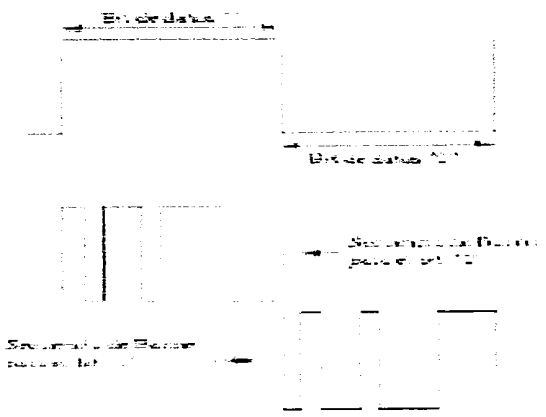


Figura 3. Codificación de la información mediante la secuencia de Barker

En Fig. 3 mostramos el aspecto de una señal de dos bits a la cual le hemos aplicado la secuencia de Barker. DSSS tiene definidos dos tipos de modulaciones a aplicar a la señal de información una vez se sobrepone la señal de *chip* tal y como especifica el estándar IEEE 802.11: la modulación DBPSK, Differential Binary Phase Shift Keying y la modulación DQPSK, Differential Quadrature Phase Shift Keying proporcionando unas velocidades de transferencia de 1 y 2 Mbps respectivamente.

En el caso de Estados Unidos y de Europa la tecnología de espectro ensanchado por secuencia directa, DSSS, opera en el rango que va desde los 2.4 GHz hasta los 2.4835 GHz, es decir, con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda total se divide en un total de 14 canales con un ancho de banda por canal de 5 MHz de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular. En el caso de

España se utilizan los canales 10 y 11 ubicados en una frecuencia central de 2.457 GHz y 2.462 GHz respectivamente.

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema si la separación entre las frecuencias centrales es como mínimo de 30 MHz. Esto significa que de los 83.5 MHz de ancho de banda total disponible podemos obtener un total de 3 canales independientes que pueden operar simultáneamente en una determinada zona geográfica sin que aparezcan interferencias en un canal procedentes de los otros dos canales. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal con el número de puntos de acceso operando en un canal que no se esté utilizando y hasta un máximo de tres canales. En el caso de España esta extensión de capacidad no es posible debido a que no existe el ancho de banda mínimo requerido (la información sobre la distribución de las frecuencias en distintas regiones del mundo se encuentra disponible en el estándar IEEE 802.11).

2.2.2 Tecnología de Espectro Ensanchado por Salto de Frecuencia (FHSS)

La tecnología de espectro ensanchado por salto en frecuencia consiste en transmitir una parte de la información en una determinada frecuencia durante un

intervalo de tiempo llamada *dwell time* y inferior a 400ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

Cada una de las transmisiones a una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal.

El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer. La ventaja de estos sistemas frente a los sistemas DSSS es que con esta tecnología podemos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

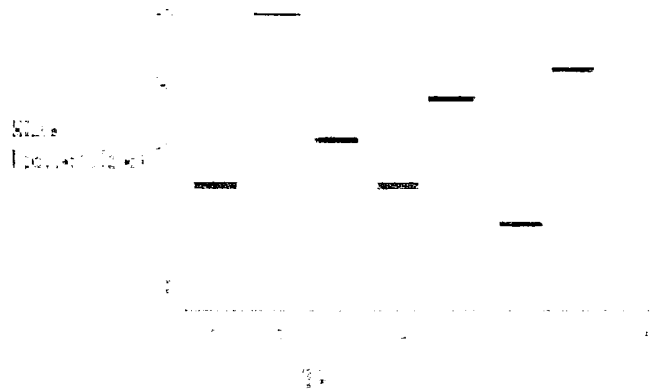


Figura 4. Modo de trabajo de la técnica FH55.

Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación el efecto global es que aunque vamos cambiando de canal físico con el tiempo se mantiene un único canal lógico a través del cual se desarrolla la comunicación.

Para un usuario externo a la comunicación la recepción de una señal FHSS equivale a la recepción de ruido impulsivo de corta duración. El estándar IEEE 802.11 describe esta tecnología mediante la modulación en frecuencia FSK, Frequency Shift Keying, y con una velocidad de transferencia de 1Mbps ampliable a 2Mbps bajo condiciones de operación óptimas también especificadas en la rma.

En este tipo de modulación la señal de información es modulada por señales de portadoras que cambian abruptamente su frecuencia a intervalos regulares, en

función directa a una señal pseudo aleatoria y modulada también con algún tipo de modulación digital para su transmisión.

2.2.3 Modalidad de Espectro Expandido OFMD (Multiplexación Ortogonal en Frecuencia)

La información que se transmite en cada banda se modula mediante OFDM. La OFDM distribuye los datos a un gran número de transportadores que están separados en frecuencias precisas. Esta separación proporciona la capacidad ortogonal en esta técnica, la cual previene que los desmoduladores detecten frecuencias distintas a la propia. Los beneficios de la OFDM son una alta eficiencia espectral, resistencia a la interferencia de radiofrecuencia y una menor distorsión de rutas múltiples.

OFDM es una tecnología de modulación digital, una forma especial de modulación multi-carrier considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad para uso tanto personal como corporativo. La técnica de espectro disperso de OFDM distribuye los datos en un gran número de carriers que están espaciados entre sí en distintas frecuencias precisas.

OFDM tiene una alta eficiencia de espectro, resilencia a la interface RF y menor distorsión multi-ruta. Actualmente OFDM no sólo se usa en las redes inalámbricas LAN 802.11a, sino en las 802.11g, en comunicaciones de alta velocidad por vía telefónica como las ADSL y en difusión de señales de televisión digital terrestre en Europa, Japón y Australia.

Al utilizar las técnicas de modulación OFDM acompañadas de las bandas múltiples, resulta más fácil recopilar energía de rutas múltiples mediante una sola cadena de radiofrecuencia y se permite que el receptor se enfrente a la interferencia de banda angosta sin tener que sacrificar sub-bandas ni velocidad de transferencia de datos. Estas ventajas están relacionadas con la capacidad de desactivar tonos concretos, así como de recuperar fácilmente tonos dañados mediante el uso del código de corrección de errores subsiguiente.

En el enfoque de OFDM de banda múltiple, el espectro disponible de 7,5 GHz se divide en varias bandas de 528 MHz. Esto permite que se implementen bandas de manera selectiva a ciertos rangos de frecuencia mientras otras partes del espectro se dejan sin usar. La capacidad dinámica de la radio para operar en ciertas áreas del espectro es importante porque puede adaptarse a las restricciones reglamentarias impuestas por los gobiernos de todo el mundo.

El enfoque de OFDM de bandas múltiples permite la coexistencia satisfactoria con los sistemas de banda angosta como las redes que siguen la norma 802.11a*, la adaptación a distintos entornos de reglamentación, la escalabilidad futura y la compatibilidad con sistemas anteriores. Este diseño permite que la tecnología cumpla con los reglamentos locales al desactivar de forma dinámica ciertas sub-bandas y tonos individuales OFDM a fin de cumplir con las reglas locales de operación en el espectro asignado.

Fig. 5 El espectro de OFDM se traslapa

3. DISPOSITIVOS Y TOPOLOGÍAS

LIMITACIÓN DE LA PROPAGACIÓN DE RF

La direccionalidad y ganancia de una antena constituyen dos características fundamentales a la hora de determinar el área de cobertura requerida. Una antena omni-direccional radia a 360 grados, en tanto las direccionales limitan la cobertura a zonas con mayor definición (Fig.13).

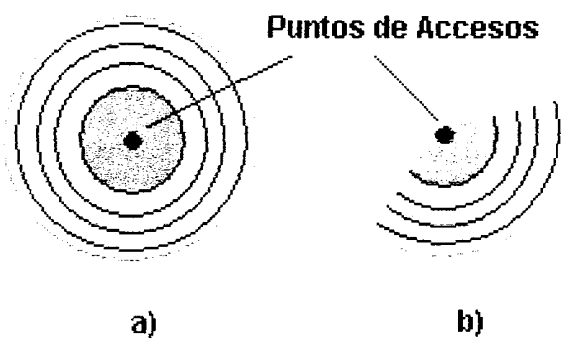


Figura 6. Patrones de radiación, (a) Omni-direccional, (b) Direccional.

La relación ganancia-transmisor de la antena se encuentra estrictamente regulada y limita el área que legalmente puede ser cubierta por un solo AP. Cuando se diseña una red inalámbrica, se requiere considerar la características de la región (cualidades físicas del entorno, locales de interés comercial cercanos o distantes,

ajenos o vinculados a la empresa, requerimientos económicos, entre otros) así como también analizar el patrón de propagación y potencia efectiva de las antenas que se empleen.

Teniendo en cuenta que las normas inalámbricas explotan las bandas media y alta ISM, sin requerimiento de licencias, se hace de esto una ventaja que actúa a su vez de atractivo para otras tecnologías y perjudicial para las redes de radio, las que son víctimas de la interferencia con otros sistemas o dispositivos inalámbricos que también basan su funcionamiento en esta área específica del espectro.

Un atacante con recursos podría estar usando transmisores de alta potencia, antenas de alta ganancia, y/o receptores más sensitivos, logrando alcanzar límites que no le son autorizados.

Cada aspecto anteriormente analizado, puede afectar el rango efectivo físico de una red inalámbrica. Luego de ser prevenido estos puntos de debilidad, es entonces que comienzan a jugar un papel fundamental las normas y software afines a la seguridad de redes.

3.1 AP (Access Point)

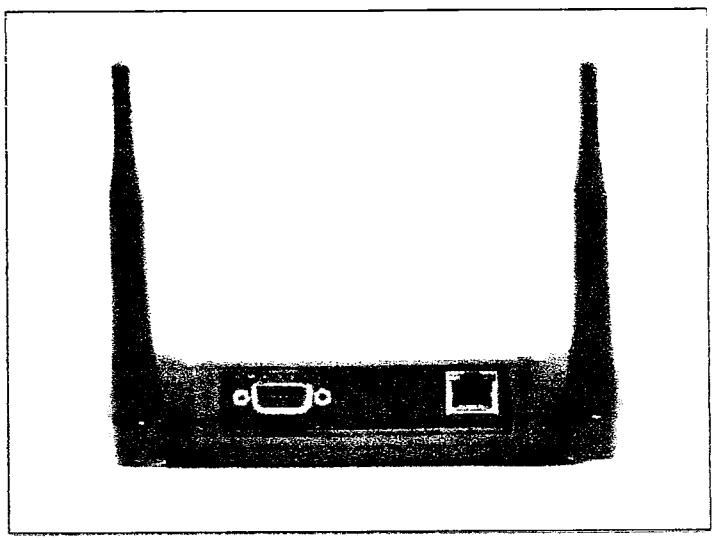


Figura 7. Access Point

Este dispositivo es el punto de acceso a la LAN cableada. Es decir, es la interfase necesaria entre una red cableada y una red inalámbrica, es el traductor entre las comunicaciones de datos inalámbricas y las comunicaciones de datos cableadas.

3.2 CPE (Customer Premise Equipment)

Es el dispositivo que se instala del lado abonado o subscriptor. Así como las tradicionales placas de red que se instalan en un PC para acceder a una red LAN cableada, las Tarjetas de Red Inalámbricas dialogan con el Access Point (AP) quien hace las veces de punto de acceso a la red cableada. La Tarjeta de Red Inalámbrica puede ser de distintos modelos en función de la conexión necesaria a la computadora:

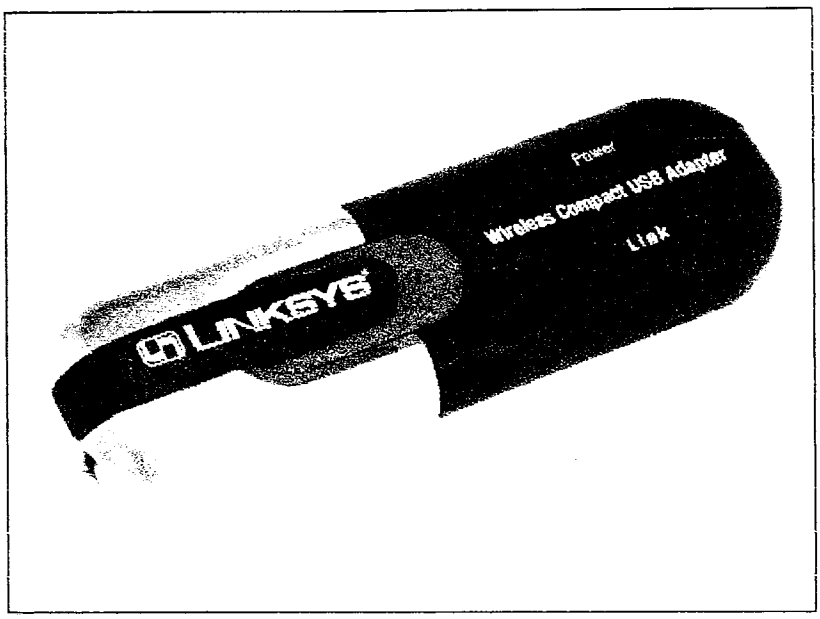


Figura 8. Tarjeta inalámbrica puerto USB

Tarjeta de Red Inalámbrica USB cuando la conexión a la computadora se realiza a través del puerto USB de la misma.

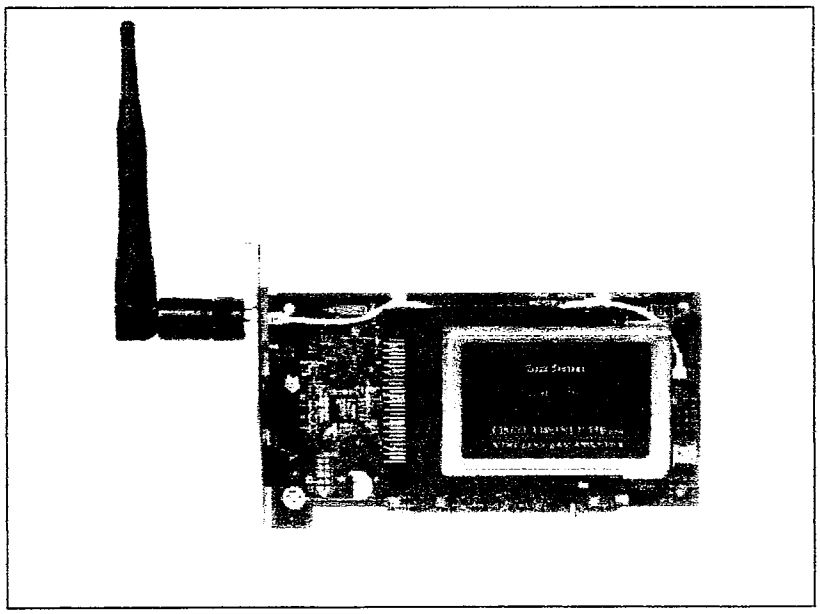


Figura 9. Tarjeta inalámbrica slot PCI

Tarjeta de Red Inalámbrica PCI cuando la conexión a la computadora se realiza a través de su slot interno PCI.

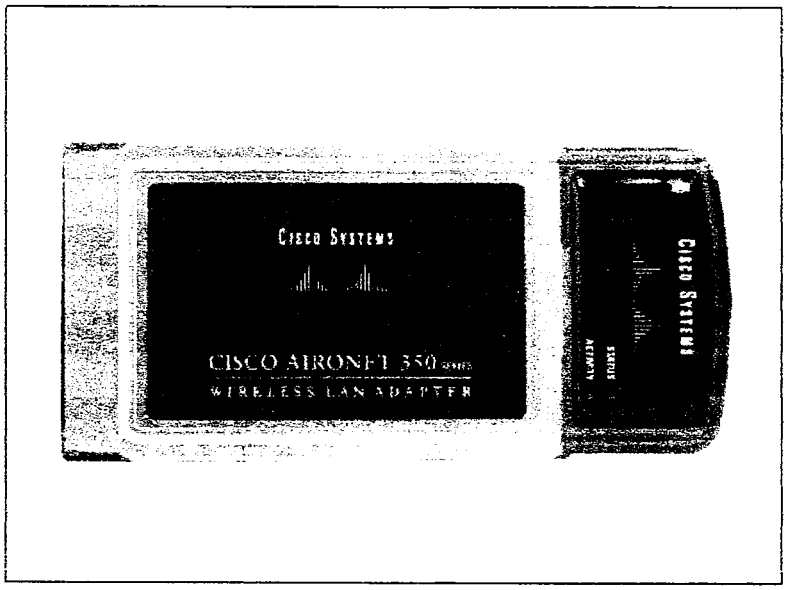


Figura 10. Tarjeta inalámbrica slot PCMCIA

Tarjeta de Red Inalámbrica PCMCIA cuando la conexión a la computadora (comúnmente laptops o notebooks) se realiza a través de su slot PCMCIA.

Típicamente un sistema 802.11 se compone de 1 Access Point y de tantos CPE como computadoras deseamos conectar en forma inalámbrica a una LAN cableada.

En las Aplicaciones Indoor puede suceder que con el fin de incrementar el área de servicio interno en un edificio es necesario la instalación de más de 1 Access Point. Cada access point cubrirá un área de servicio determinada y las computadoras tomaran servicio de LAN a través del Access Point más cercano.

En las aplicaciones de Internet Inalámbrica Outdoor puede darse el caso que la cantidad de abonados CPE sea elevado y debido al alto tráfico que ellos generan se requiera instalar más de un AP (Access Point) con el fin de poder brindar servicio de alta calidad.

En estas aplicaciones, con el fin de mejorar el área de cobertura, puede instalarse en el nodo central un amplificador bidireccional a tope de torre.

3.3 SERVICIOS

En las redes inalámbricas de área local, se definen un conjunto de servicios según las aplicaciones IEEE 802.11, entre los que encontramos fundamentalmente los siguientes:

- *Asociación:* se establece una asociación primaria entre una estación y un punto de acceso.
- *Reasociación:* se habilita una asociación establecida y se transfiere de un punto de acceso a otro posibilitando la movilidad de las estaciones.
- *Disociación:* se notifica desde una estación o un punto de acceso que la asociación ya existente finaliza.
- *Autentificación:* se establece la identidad de una estación a cada una de las otras con las que desea comunicarse.

- *Desautentificación:* finaliza el estado de autentificación preestablecido.
- *Privacidad:* se protege el contenido de los mensajes para que estos no sean leídos por interceptores.
- *Integración:* conexión entre una red WLAN con otras LAN cableadas o no.

3.4 ARQUITECTURA EXTERNA

El grupo de trabajo 802.11 ha desarrollado un modelo de arquitectura externa definido por dos conceptos fundamentales: *Grupo de Servicio Básico (BSS)* y *Grupo de Servicio Extendido (ESS).*

El *Grupo de Servicio Básico* consiste en un número determinado de estaciones que compiten por acceder al mismo medio compartido, ya sea de forma independiente (Fig.10a) o a un punto de acceso conectado a un sistema de distribución determinado según el modelo cliente/servidor (Fig.10b). El grupo de servicio básico independiente (IBSS) no requiere de un AP, en cuyo caso, estamos en presencia de una red LAN inalámbrica *ad hoc.*

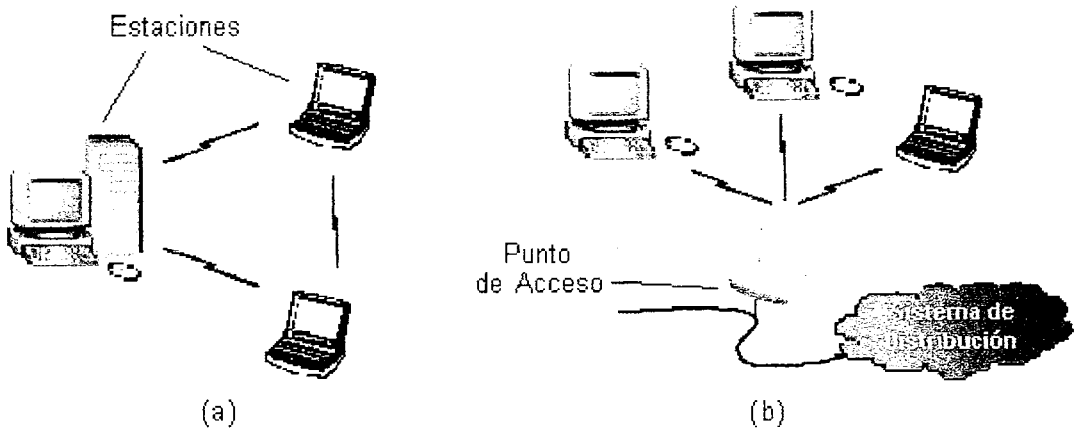


Figura11. Grupos de Servicio Básico, (a) Independiente, (b) a través de un punto de acceso.

El *Grupo de Servicio Extendido* es la clasificación de dos o más grupos de servicio básico interconectados por un sistema de distribución determinado (Fig.11).

Figura 12. Grupo de Servicio Extendido formado por dos grupos de servicio básico.

3.4.1 Topología ad hoc

Las redes ad hoc son consideradas estructuras de interconexión entre dos o más dispositivos inalámbricos, en ausencia de un punto de acceso y con un tiempo de existencia limitado dada la movilidad de sus miembros constituyentes, razón por la cual son clasificadas como grupos de servicio básico independientes (Fig.10a).

Estas redes de radio ofrecen ventajas en el intercambio de datos homólogo-a-homólogo (peer-to-peer) entre los nodos que la conforman. Uno de sus beneficios está estrechamente relacionado con su característica fundamental, cada nodo tiene la capacidad de encaminar las tramas de comunicación hacia sus vecinos.

Dado que las topologías ad hoc están propensas a cambios estructurales constantes, las conexiones son alcanzadas examinando continuamente el estado de la red (encaminamiento proactivo), chequeando su estado actual en caso de existir tráfico para ser transmitido (enrutamiento reactivo) o una combinación de estos dos métodos.

El enrutamiento proactivo requiere de un uso exhaustivo del ancho de banda, característica que lo diferencia del modo reactivo. La selección del método más idóneo (entre dos extremos) depende mucho de la aplicación, la configuración y el contexto del servicio.

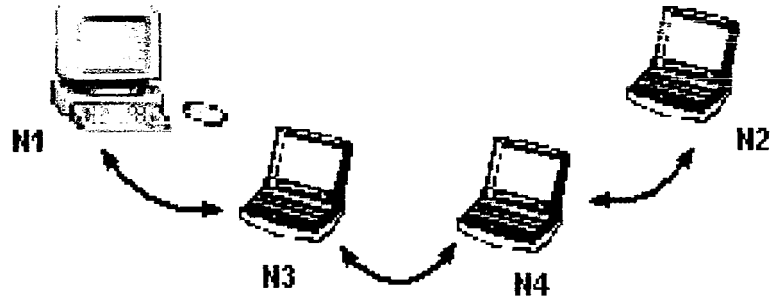


Figura. 13. Enrutamiento en una red ad hoc sencilla.

Observando en Fig. 12, podemos notar como es improbable que el nodo 1 pueda establecer una comunicación directa con los nodos 3 y 4. Para realizar un intercambio de tráfico entre ellos, debe utilizar al nodo 2 (y 3 en caso de establecer una comunicación con el nodo 4) como mediador, dado que este si entra dentro de su radio de acción. En esto esencialmente consiste el modo de funcionamiento de una red ad hoc.

3.4.2 Topología de Infraestructura

Este tipo de red se extiende de una existente de cable para incorporar dispositivo inalámbrico a una estación base, denominado PUNTO DE ACCESO.

El punto de acceso es el encargado de unir la red LAN inalámbrica y la red LAN con cables sirve de controlador central de la red LAN inalámbrica.

El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión especifica .La extensión y el número de dispositivos dependen del estándar de conexión inalámbrico que se utilice y del producto.

Si la zona es grande por lo general hay varios puntos de acceso lo que significa que hay varias estaciones base, en cambio si la zona es pequeña como puede ser un hogar o una pequeña oficina con un solo punto de acceso bastaría

4. SEGURIDAD EN REDES IEEE 802.11

Debido al aumento progresivo en la productividad y la creciente popularidad de las comunicaciones inalámbricas de forma general, es que se ha hecho necesario diseñar una arquitectura sólida, con énfasis en la seguridad para ofrecer mayor confiabilidad a los que soliciten estos servicios.

Previo a decidir que medida de seguridad se implementará, es de vital importancia realizar un estudio de radio-propagación para los AP a instalar en la red WLAN. Se requiere restringir la cobertura a la zona de interés, ya que con una correcta combinación antena-transmisor podemos evitar extender el área de acceso a lugares ajenos a nuestros propósitos.

El estándar IEEE 802.11 sujeta otras disímiles características de seguridad, tales como *autentificación en sistema abierto* y de *clave pública*, el *Identificador de Grupo de Servicios* (*SSID* de inglés Service Set Identifier), y el *Equivalente a Privacidad Cableada* (*WEP* del inglés Wired Equivalent Privacy). Estos aspectos se diferencian en el grado de confiabilidad. Cada uno de ellos han sido objetos de estudios en la seguridad de redes, y muestran cierto nivel de vulnerabilidad ante los ataques de intrusos.

La vulnerabilidad del protocolo WEP ha sido estudiada y demostrada teóricamente por un grupo de estudio en la seguridad de redes inalámbricas, de la Universidad de Berkeley, California, los que han publicado una serie de artículos conocidos como "Berkeley Paper", que exponen a detalle las fragilidades del algoritmo criptográfico RC4 y de la forma en la que es usado en el estándar 802.11.

Con el fin de mejorar las debilidades de las técnicas empleadas, la IEEE define el estándar 802.1x, el cual promueve una fuerte y más flexible seguridad que la autentificación y los mecanismos de encriptación. Lamentablemente, la implementación del WEP no posee los requerimientos de seguridad para las más grandes empresas y algunas organizaciones medias, muy vulnerables a las agresiones por aquellos que desean adquirir por aire, los datos de interés de estas compañías.

Es evidente el constante desarrollo de la tecnología y con él, el mejoramiento constante de los métodos de seguridad en este tipo de redes. El estándar 802.1x ha sido objetivo de estudio y víctima de ataques que han manifestado sus debilidades. En su lugar, surgen otros nuevos como el Acceso Protegido Wi-Fi (WPA del inglés Wi-Fi Protected Access) y una versión mejorada del mismo reconocida como IEEE 802.11i o WPA2.

Es primordial considerar, antes de implementar cualquier otra medida de seguridad, las implicaciones de la propagación de radiofrecuencias (RF) por los puntos de acceso en una red de radio. Logrando una inteligente combinación antena-transmisor, evitaremos extender el área de cobertura a otros puntos carentes de interés.

4.1 AUTENTIFICACIÓN

Previo a la asociación de una estación con su AP correspondiente, se ejecuta el servicio de autentificación subdividido en dos tipos: *sistema abierto* y *clave pública.* La primera consiste básicamente en una elemental solicitud de autentificación que identifica a la estación. En caso de no existir dificultades, las estaciones involucradas en la comunicación, quedan autentificadas. La segunda adquiere sentido cuando las estaciones implicadas, comparten la misma clave pública, transmitida a ellas a través de un canal seguro no considerado dentro del medio inalámbrico. En la encriptación interviene un texto originado por el

Generador de Números Pseudo-aleatorios (PRNG del inglés Pseudo Random Number Generator) enviado desde el AP a la estación, la cual debe encriptarlo con la clave pública y posteriormente enviar el resultado al AP. Este se encarga del proceso de desencriptación y compara el producto con el texto original, en caso de compatibilidad, la conexión ha sido exitosa en un sentido. El mismo procedimiento se repite en dirección inversa.

A pesar del proceso aparentemente seguro llevado a cabo, los ataques más frecuentes a redes WLAN consisten en la captura de la clave pública a partir de un texto encriptado.

4.2 IDENTIFICADOR DEL GRUPO DE SERVICIO

El *Identificador del Grupo de Servicio* (*SSID*) fue definido como un seudónimo de red que identifica el perímetro de cobertura de uno o más puntos de accesos. Se definen esencialmente dos modos de trabajo:

- El AP transmite periódicamente su SSID correspondiente y cada estación terminal se asociará a él, dentro del área perimetral, según lo desee, apoyándose en el identificador proporcionado.
- El AP, como medida de seguridad, no transmite el SSID, por lo que cada estación terminal que desea asociarse a su AP correspondiente, deberá tener previamente configurado el mismo SSID.

Desafortunadamente este modo carece de seguridad, si tomamos en cuenta que las tramas de administración se transmiten de forma abierta en las redes WLAN 802.11. Un intruso puede interceptar estas tramas y descubrir el SSID del punto de acceso.

4.3 EQUIVALENTE A PRIVACIDAD CABLEADA (WEP)

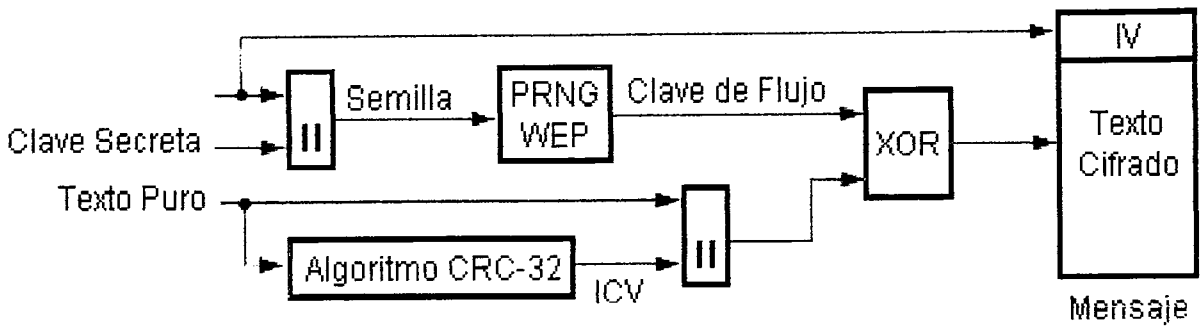
El estándar IEEE 802.11 define protocolo WEP en el intento de proveer una conexión tan confiable como la equivalente en comunicaciones cableadas, usando un chequeo redundante cíclico (CRC) para asegurar el cuerpo de datos y el algoritmo simétrico RC4 para la encriptación y desencriptación.

Algoritmo de Encriptación

Varios esquemas y algoritmos de encriptación son usados en diferentes WLAN, según los intereses de la organización. WEP usa el flujo cifrado RC4 como algoritmo criptográfico el cual depende básicamente de los siguientes parámetros:

- Vector de inicialización IV, número aleatorio público disponible, con un máximo de 24 bits.

- Clave Secreta de 40 bits, la cual pude ser única para cada usuario o compartida entre todos o un grupo de ellos.
- Valor Íntegro de Chequeo ICV de 32 bits.
- Clave de Flujo[1] lo más compleja posible, utilizada en la transformación del texto puro[2] del mensaje en una forma relativamente indescifrable llamada texto cifrado.



IV Vector de Inicialización (Initialization Vector)
ICV Valor Íntegro de Chequeo (Integrity Check Value)

Figura 14. Encriptación WEP.

Posterior al mecanismo CRC-32[3] en la obtención del ICV, el extremo transmisor debe encriptar el mensaje antes de ser enviado al AP o a cualquier otro dispositivo inalámbrico.

[1] Clave de flujo, del inglés "keystream" o "key sequence".
[2] Texto puro o plano, del inglés "plaintext" referido a la carga útil (payload).
[3] Variante CRC empleada por el protocolo WEP para obtener el ICV de 32 bits.

Como se observa en Fig. 14, el algoritmo RC4 destina la clave secreta (40 bits) y el vector IV (24 bits) para obtener una semilla[4] de 64 bits, producto de entrada del bloque PRNG. Este último es el encargado de generar una secuencia extendida de bytes pseudo aleatorios denominada clave de flujo. Al texto original del mensaje se le aplica una función CRC para obtener el ICV de 32 bits. Este es combinado con el mismo texto puro y el resultado es aprovechado conjuntamente con la clave de flujo en una función lógica OR exclusivo (XOR) para dar origen al texto cifrado.

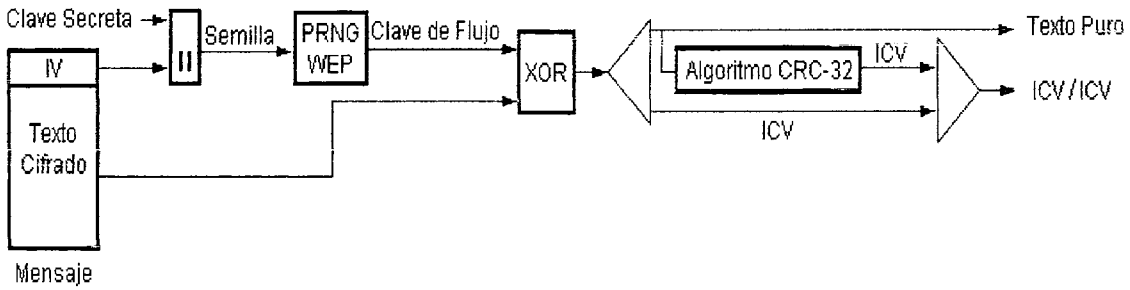


Figura 15. Desencriptación WEP.

Para el proceso de desencriptación el vector IV procedente del mensaje recibido, es usado para generar la clave de flujo que ayudará a desencriptar el texto. Combinándola con el texto cifrado obtenemos el texto plano y el ICV. El proceso de desencriptación es comprobado a través del algoritmo de chequeo, que recibiendo el texto original proporciona el valor de ICV, el cual es comparado con

[4] Semilla, referida al término inglés "seed".

el ICV transmitido. En caso de ser diferente los valores de chequeo, el mensaje recibido está errado (Fig. 15).

Debilidades

El grupo de estudio de seguridad en redes inalámbricas 802.11, en la Universidad de Berkeley, ha demostrado que es posible realizar una modificación adecuada al cuerpo original del mensaje y el extremo receptor estar ajeno a tal intromisión, por lo que este pudiera comprometer la funcionalidad del algoritmo CRC por inserción de bits en el mensaje y el receptor no reconocer alguna dificultad hasta que haya sufrido un problema del que la encriptación y el procedimiento CRC debieron haberla protegido. Esto implica además, la posibilidad de redireccionar el tráfico. En caso de que un intruso capture un dato durante la transmisión y modifique la dirección IP de envío, cualquier respuesta al paquete solicitado, será enviada al interceptor y no al cliente que lo originó.

Desafortunadamente el estándar 802.11 no especifica un método para proveer a cada usuario de claves diferentes. Si una empresa emplea una clave secreta para todos sus usuarios, el IV debe explotar cada valor posible, de lo contrario la clave de flujo será redundante y de fácil deducción. Este estándar tampoco especifica los pasos necesarios para lograr una entrada de componentes aleatorios (clave e IV) y dar como resultado una clave de flujo lo más compleja posible. Una longitud

de 24 bits para el vector IV es relativamente insuficiente dado que este se repetirá cada cierto tiempo de transmisión continua para diferentes paquetes, facilitando oportunidad de descubrir la clave. Partiendo de que este estándar cuenta únicamente con 2^{24} posibles combinaciones de IV, todo valor disponible único será consumido en menos de un día.

Si un intruso adquiere la clave de flujo que encriptó un mensaje, necesitará solamente revertir el proceso para adquirir el texto original.

Para incrementar el nivel actual de seguridad en una infraestructura, se puede considerar las siguientes propuestas:

- Emplear un software de seguridad (firewall) para separar la red inalámbrica de una red cableada (Fig.16).
- Implementación de una estructura de generación dinámica de claves.

- Invocar a un mecanismo de autentificación mutuo entre el dispositivo inalámbrico y el servidor.

- Usar zonas seguras en la INTRANET, con el uso de firewalls, servidores de control de acceso y filtradores de paquetes, para separar la red inalámbrica del tráfico (Fig.16).

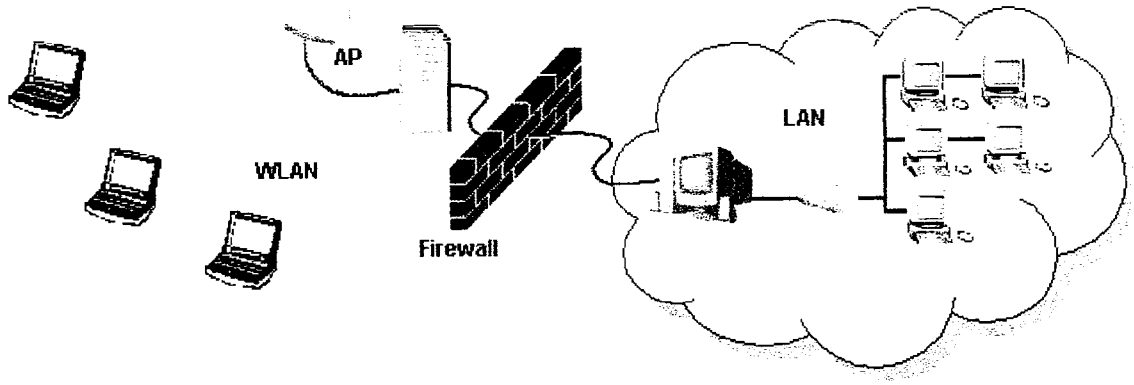


Figura 16. Separación de una Intranet en zonas. Uso del firewall.

4.3.1 Estándar 802.1x

Esta norma se encarga con mayor seriedad y directamente de las debilidades del estándar 802.11. Provee un método para la autenticación y autorización de conexiones a una red inalámbrica bloqueando toda gestión de red mientras no haya una correcta certificación. Sus características lo convierten en una idea alternativa en la seguridad de este tipo de redes. Asimismo, posibilita el uso de dispositivos de diferentes proveedores sin realizar cambios trascendentales en el estándar original 802.11.

Emplea el algoritmo RC4 para la encriptación del mensaje con una clave de 128 bits, con la cual previene de los ataques pasivos a la red. De igual forma, el sistema será capaz de gestionar y rotar las claves de encriptación por cada sesión.

IEEE 802.1x incorpora el uso de dos nuevos protocolos EAP y RADIUS.

4.3.2 Protocolo de Autentificación Extensible (EAP)

El Protocolo de Autentificación Extensible (EAP, del inglés Extensible Authentication Protocol) es una extensión del ya conocido PPP (Point-to-Point Protocol) proveedor de un método estándar de transporte para enlaces "punto a punto". EAP proporciona un mecanismo para aceptar métodos de autentificación adicionales junto a PPP. Esta norma de seguridad consiste, básicamente, en guiar un mensaje EAP por una LAN cableada o no, empaquetándolos en tramas Ethernet en ausencia del protocolo PPP. De aquí que la 802.1x se denomine *EAP over LAN* (EAPOL), usualmente definido para redes LAN Ethernet cableadas o inalámbricas 802.11, y además extendida a las Token-Ring y FDDI.

Se introduce, igualmente, el concepto RADIUS (del inglés Remote Authentication Dial-In User Service), protocolo destinado al servicio de usuario para una autentificación remota y diseñado según los criterios del marco AAA.

El protocolo RADIUS implementa la autentificación, autorización y contabilización para las conexiones a servidores. Empleando un servidor RADIUS no es necesario almacenar información de usuarios en cada AP de la red inalámbrica, por lo que se logra una administración y configuración relativamente sencillas.

Existen diferentes tipos de protocolos EAP (Fig.17):

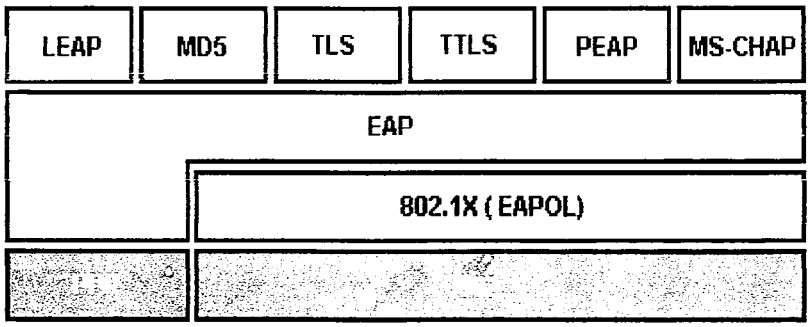


Figura 17. Ubicación del protocolo EAP.

- **LEAP** (*Lightweight EAP*): Es empleada en redes WLAN. Con LEAP es necesaria una autenticación mutua tanto del cliente como del servidor (típicamente un servidor RADIUS). Se utilizan claves privadas compartidas para construir los mensajes intercambiados. Soporta plataformas *Windows, Macintosh* y *Linux*. Fue patentado por *Cisco*.

- **EAP-MD5** (*EAP–Menssage-Digest5*): Método de autenticación por desafío. El servidor envía un mensaje "desafío" al cliente que quiere ser autentificado. El cliente debe responder a la petición con otro mensaje MD5 o con un mensaje rechazando la autentificación. Es el más sencillo de implementar pero el menos fiable ya que sólo autentifica al cliente frente al servidor, no al servidor frente al cliente.

- **EAP-TLS** (*EAP–Transport Level Security*): Proporciona autenticación mutua, negociación cifrada e intercambio de claves entre extremos. Soporta fragmentación y reensamblaje de mensajes. Este

protocolo está destinado a redes cableadas y depende de certificados. Necesita que los extremos que establecen el intercambio para la autentificación tengan su propio certificado. Fue desarrollado por *Microsoft*.

- **EAP-TTLS** (*EAP-Tunneled TLS*): No necesita que ambas partes estén certificadas, solo requiere la certificación del servidor de autentificación. En el intercambio inicial de mensajes, se utiliza el nombre y la clave del usuario y una vez realizada la autenticación, se crea un túnel que se utiliza para intercambiar información segura. Consta de parámetros pre-configurados para el cliente WLAN, lo que lo hace más atractivo. Fue desarrollado por *Funk Software* y *Certicom*.

- **PEAP** (*Protected EAP*): Similar a EAP-TTLS. No especifica ningún método de autenticación, pero proporciona canales seguros para otros protocolos de autenticación. Fue desarrollado por *Microsoft, CISCO* y *RSA*.

- **MS-CHAP:** Protocolo de *Microsoft* de autenticación por desafío mutuo, también reconocido como MS-CHAPv1, ya que se cuenta con una segunda versión (MS-CHAPv2) más moderna que resuelve varios problemas de la primera.

4.4 ACCESO PROTEGIDO WI-FI

Según habíamos examinado anteriormente, una clave de 40 o 128 bits es insuficiente afines a la autentificación y encriptación. La Alianza Wi-Fi recientemente aprobó un nuevo estándar de seguridad reconocido como Acceso Protegido Wi-Fi (WPA del inglés Wi-Fi Protected Access) dirigido directamente a las vulnerabilidades de las redes inalámbricas, ahora con una mayor seguridad independientemente del entorno heterogéneo, típico en empresas surtidas por proveedores diferentes y en lugares visitados por clientes inalámbricos con disímiles características técnicas.

Esta compatibilidad se ha certificado en productos de organizaciones tan prestigiosas como *Atheros Communications, Broadcom Corp., Cisco Systems, Intel Corp., Intersil,* y *Symbol Technologies* y a su vez dispensadas por proveedores como *D-Link, Linksys, Netgear, SMC, 3Com.*

El protocolo WPA es una combinación de la ya existente estructurta de autentificación (802.1x con el protocolo EAP), un robusto esquema de encriptación denominado Protocolo de Integralidad de Clave Temporal (TKIP, del inglés Temporal Key Integrity Protocol) y un Verificador de Integridad de Mensaje (MIC, del inglés Message Integrity Checker), para evitar que los paquetes sean falsificados.

Cuando WPA se habilita, una tarjeta de usuario intenta asociarse a su punto de acceso correspondiente. El AP bloquea el acceso a la red inalámbrica hasta que las credenciales de usuario sean aprobadas por el servidor de autentificación (servidor RADIUS). Después de aceptar las credenciales, el servidor RADIUS produce una única clave de sesión de 128 bits que TKIP distribuye al usuario y al AP. Luego, el usuario se asocia a la red y WPA establece un mecanismo de administración de clave, generando automáticamente una diferente para cada paquete transmitido.

Para los consumidores y organizaciones más pequeñas que no invierten en servidores RADIUS, este protocolo proporciona una clave de sesión pre-compartida[5], esencialmente una contraseña. Luego se generan claves por paquetes automáticamente y se facilita un mecanismo de chequeo de integridad de mensaje capaz de determinar si cualquier paquete se ha alterado durante una sesión. Los usuarios también consiguen una potente encriptación de TKIP.

WPA realmente constituye el primer paso hacia una potente seguridad en las redes de radio. En este mismo año, la IEEE publica otra norma de seguridad llamada 802.11i, también conocido como WPA2, que añade el Estándar de Encriptación Avanzada (AES, del inglés Advanced Encryption Standard), un fuerte método de encriptación para datos privados.

5. EVOLUCIÓN DEL MERCADO

El mercado de las soluciones inalámbricas alcanzó en el año 2002 un volumen de negocio de unos 1.600 millones de dólares y según todas las previsiones, se espera que experimente un crecimiento anual del 20%, a pesar de algunos factores en su contra que frenan este desarrollo como los problemas de seguridad y la diversidad de estándares.

Y es que la preocupación por la seguridad es uno de los problemas que más tienen en cuenta las compañías, junto con las restricciones presupuestarias. A medida que la economía se vaya recuperando y los nuevos estándares incluyan características de seguridad mejorada, el mercado crecerá, por lo que se espera que en el año 2006 se alcance un volumen de 2.600 millones de dólares.

Otro de los factores negativos es que en este momento se está produciendo un retraso en el proceso de ratificación de los nuevos estándares. Este proceso, en el caso del 802.11i está siendo más caro y lento de lo que los fabricantes calcularon, por lo que hasta finales de 2003 o principios de 2004 este estándar no se lanzará al mercado.

[5] Clave de sesión pre-compartida, del inglés preshared session key (PSK)

Por otro lado, muchas compañías se han lanzado ya a comercializar soluciones que soportan el estándar 802.11g, aunque todavía no está definido del todo. Las primeras pruebas con este tipo de equipos han demostrado que la interoperabilidad presenta lagunas, y que en redes híbridas, las prestaciones tienden a caer a los niveles del estándar anterior.

Se espera que el crecimiento venga impulsado por la tecnología Wi-Fi, así como por la mayor presencia de las tarjetas multiprotocolo, capaces de operar en estándares diversos como el 802.11a, b y g. De hecho, en Estados Unidos esto ya se está produciendo ya que el protocolo 802.11b, convive con el 802.11a, que ofrece un mayor ancho de banda. Además, esta opción tiene la ventaja de proteger las inversiones de la obsolescencia y permite administrar el ancho de banda en función del uso o localizaciones.

Por último podemos decir que tanto la mejora de las redes como una mayor capacidad permitirán montar redes con dispositivos-clientes móviles siempre conectados, de igual manera a como sucede en las redes móviles de 2.5G GSM/GPRS, al tiempo que habrá un despliegue de Web Services para aplicaciones móviles.

Así mismo se tendrán en cuenta las facilidades y ventajas de estas tecnologías van a hacer posible la rápida expansión de estas aplicaciones móviles como por ejemplo la ubicuidad, la incorporación a los PC de tecnología Wi-Fi de serie, la

mejora de los estándares de seguridad, etc. Y una tendencia importante sería la aparición de una plataforma de conmutación centralizada que integra capacidades para gestionar la seguridad, la administración de la red y la calidad de servicio.

En cuanto a las tendencias tecnológicas se está trabajando con el fin de ofrecer soluciones inalámbricas con puntos de acceso más ligeros y económicos y con una plataforma que permita controlarlos de forma centralizada, además de incorporar otras funcionalidades.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o esta prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

El fenómeno asociado al termino "inalámbrico", es decir, no tener que instalar mas cables además de los de la red de telefonía y la red de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes domesticas y la experiencia de conexión desde el hogar.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN Inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y NIC inalámbricas.

Esto permite al usuario viajar a distintos lugares sin perder el acceso a los datos de la red.

6. DESCRIPCIÓN DE LA EMPRESA

Empresa Comercializadora y distribuidora de productos de alta tecnología, además de la prestación de servicios y mantenimiento técnico de los equipos; cuenta con el respaldo de Alkosto empresa de capital 100% Colombia.

La compañía está especializada en comercializar productos de consumo masivo, haciéndolos llegar a los principales canales de comercio, prestando excelentes servicios de venta a sus Clientes y proporcionando satisfacción a sus Proveedores por la distribución de sus productos e investigar los métodos para lograr la mayor eficiencia en distribución; y en interrelacionar todos los procesos para alcanzar la Excelencia en el Servicio.

6.1 NECESIDAD

Incrementar las ventas por medio de muestras virtuales a nuestros visitantes utilizando tecnología de comunicación inalámbrica Blueto oth, Intel Centrino, Airport Extreme.

Como complemento a la necesidad se utilizara los diferentes equipos habilitados para esta tecnología para que los clientes interactúen con los mismos (Show Room)

6.2 ÁREA

Anexo 1

280 Metros Cuadrados del Punto de Venta

Divididos en 5 categorías a saber:

1. Home Cinema
2. T.V. – Video (LCD, Plasma, Televisión, Retroproyecto, DLP)
3. Audio (Car – Audio, Microcomponentes, Equipos)
4. Video Cámaras y Fotografía
5. Office (Desktops, Notebooks, Impresoras, Multifuncionales, Scanners, PDA's)

6.3 MAQUINAS

Inicialmente se va a trabajar con los siguientes equipos:

- 8 Computadores Con Procesadores Intel Pentium IV y Amd Athlon XP
- 11 Portátiles HP Con Tecnología Intel Centrino

- 8 PDA's (PALM – iPAQ)
- 3 Impresoras con comunicación Infrarroja
- 2 Multifuncionales con comunicación Infrarroja
- 3 Cámaras digitales con Tecnología Bluetooth o infrarroja
- 3 Mac's con Procesadores G4 y tecnología Wi – FIRE

Se van compartir, Imágenes, Videos, Audio, Archivos varios, animaciones en flash.

6.4 SEGURIDAD

- Ktronix cuenta con un programa anti Spam
- Los usuarios del sistema tienen claves alfanumericas de 8 digitos.
- Deacuerdo al rango de cada usuario se manejan las restricciones para ingresar a las aplicaciones y datos
- Se tiene un control de acceso a Internet
- Actualmente Ktronix utiliza el Software HotFix

7. PROPUESTA

Para el diseño de la propuesta se tuvieron en cuenta las necesidades y requerimientos de la empresa, esta se basa en los estándares establecidos para su implementación y para los componentes a ser utilizados, de acuerdo al tamaño

y tipo de información que se utiliza en la compañía, se propone un diseño de red con varias opciones teniendo en cuenta una relación costo-beneficio, que reúne las características técnicas para ofrecer una solución a las necesidades planteadas con una proyección que permitirá expandirla hacia nuevas tecnologías y nuevos servicios, como se describen a continuación.

7.1 PRIMERA PROPUESTA

Esta primera propuesta es la mas económica, incluye un AccesPoint D-Link y 8 Tarjetas de Red PCI Inalámbricas D-Link para los equipos Intel Pentium IV y AMD Athlon XP que no vengan habilitados para la comunicación inalámbrica.

Cantidad	Descripción	Precio
1	**Enrutador Inalámbrico D-Link 624+** Air Plus, de Banda Ancha, "High Speed 2.4Ghz" 802.11**G**, 108Mbps, 4 puertos full duplex 10/100 switche, es punto de acceso inalámbrico, y permite compartir conexión a internet de alta velocidad, por cable o ADSL. Compatible con 802.11b.	 $ 250.000
8	Tarjeta de red **Inalámbrica D-Link DWL-G520** Air Plus Xtreme Wireless-G PCI Adapter para los PC de escritorio para redes inalámbricas clase **"G"** (802.11G)con alcance de 50Mts. Velocidad de transferencia 108 Mbps, full compatible con las redes WI-FI (802.11B).	

		$ 140.000
	TOTAL	**$ 1.370.000 incluido 16% IVA**

Tabla 2. Cotización 1

Esta opción es muy buena para empezar, pues incluye equipos de alta tecnología muy fáciles de configurar y utilizar y se constituye en la mejor opción Precio – Rendimiento.

7.2 SEGUNDA PROPUESTA

En esta propuesta Tenemos un AccesPoint D-Link Doble Banda (2.4 GHz / 5 Ghz) que nos ofrece un mejor desempeño libre de cualquier clase de interferencias, y 8 tarjetas de red inalámbricas USB Linksys Plug & Play , con un alcance máximo de 50 metros nos permite configurar cualquier computador o portátil que tenga puertos USB y no venga habilitado para comunicaciones inalámbricas en minutos, sin necesidad de destaparlos, es una muy buena opción de alto rendimiento y facilidad de configuración.

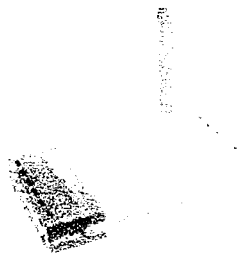
Cantidad	Descripción	Precio
1	**Enrutador Inalámbrico D-Link DI-784+** Air Premier, de Banda Ancha:Cable/DSL, "High Speed 2.4/5Ghz", doble Banda; A y G 802.11A/**G**, 108Mbps, Switche de 4 puertos full duplex 10/100, es punto de acceso inalámbrico, y permite compartir conexión a internet de alta velocidad, Compatible con 802.11b. Soporta las 3 frecuencias.	 $ 590.000
8	Tarjeta de red Inalambrica Linksys WUSB54G Wireless-G USB 2.0 Adapter, para toda clase de PCs con puerto USB. Para redes inalambricas clase **"G"** (802.11G)con alcance de 50Mts. Velocidad de trasferencia 54 Mbps, full compatible con las redes WI-FI (802.11B).	 $ 280.000
	TOTAL	**$2.830.000 incluido 16% IVA**

Tabla 3. Cotización 2

7.3 TERCERA PROPUESTA

Para una red inalámbrica mas segura vamos a utilizar 1 AccesPoint Cisco Aironet 1200 Wireless que esta especialmente diseñado para redes de alta Velocidad, es Fácilmente configurable, trabaja en las 2 bandas (2 Ghz – 5 Ghz) incluye soporte para Vlans, y Tarjetas inalámbricas PCI **Cisco AiroNet 350 Series** fácil de instalar, soporta encripción de 128 Bits para mantener una red segura

Cantidad	Descripción	Precio
1	Cisco Aironet® 1200 Series IEEE 802.11 a/b/g Access Point Modular, Dual Radio Platform for Single, Dual or Tri-mode Operation 5GHz Integrated Antennas 2.4- and 5GHz Diversity Antennas Cisco IOS Software Virtual LAN (VLAN) Support Downstream QoS Support Proxy Mobile IP Cisco SWAN Wireless Domain Services (WDS) Fast Secure Roaming WAN Link Remote Site Survivability Client ARP Caching RADIUS Server per SSID Two RP-TNCs for External 2.4GHz Antenna Connection 8MB Flash Memory	 $ 1.872.000
8	Cisco Aironet 350 Series Tarjeta de red inalabrica PCI para redes seguras cuenta	

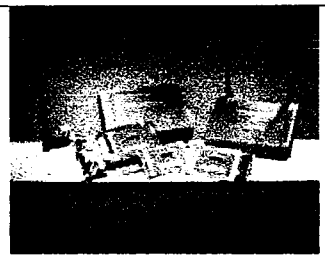
	con encripcion de 128 Bits	 $ 552.000
	TOTAL	**$ 6.288.000 incluido 16% IVA**

Tabla 4. Cotización

CONCLUSIONES

- A partir del estudio y el análisis que se realizó en el caso de KTRONIX, se dedujo que al implementar algunas de las propuestas, la empresa puede llegar a tener un mayor auge en el ámbito de las Telecomunicaciones.
- La implementación de soluciones de Red Inalámbrica nos permite disminuir los costos, ahorrar tiempo.
- La finalidad de una Red inalámbrica en KTRONIX es resolver problemas comunes, como la virtualización y demostración de los servicios de última generación en productos de comunicación que se exhiben.
- Tal vez el futuro esté por ahí, por las nuevas especificaciones, aunque creemos que a la especificación IEEE 802.11b se le puede dar aun mucho juego con antenas con más capacidad de amplificación. En la red se pueden encontrar procedimientos para fabricar Antenas caseras con botes de patatas fritas, papel platina y otros objetos cotidianos.

En los websites de los principales fabricantes de computadores podemos encontrar información sobre las nuevas tecnologías inalámbricas y sus estandares, IEEE 802.11a que nos permiten alcanzar las 54 Mbps en corto alcance y 6 Mbps en el largo alcance. Cuando tuvimos que decidir qué marca de

componentes utilizar ya conocíamos esta nueva especificación pero sólo Intel hablaba de ella y como ya hemos comentado fue imposible contactar con un proveedor de Intel con información en ese momento y lo más importante de la documentación de Intel no parecía desprenderse que estuviese permitido en Europa emitir libremente en "5 GHz UNII spectrum".

Tal vez el futuro esté por ahí, por las nuevas especificaciones, aunque creemos que a la especificación IEEE 802.11b se le puede dar aun mucho juego con antenas con más capacidad de amplificación. En la red se pueden encontrar procedimientos para fabricar Antenas caseras con botes de patatas fritas, papel platina y otros objetos cotidianos.

Bibliografía

1. Blaw, John (2002). "Wi-Fi Hotspot Networks Sprout Like Mushrooms". **IEEE Spectrum** 39(9): 18-20.

2. Borisov, Nikita; Goldberg, Ian; Wagner, David (2001). "Intercepting Mobile Communications: The Insecurity of 802.11". Universidad de Berkeley, California.
   Disponible en: http://www.isaac.cs.berkeley.edu [consultado 13/02/2004]

3. Huber, Josef (2002). "W-LAN no Threat to MNOs". **International Telecommunication** 36(9): 30-34.

4. Huckaby, Tim (2001). "Is 802.1x the Answer? ". **Windows 2000 Magazine** 7(16): 50.

5. Levillain, Philippe (2002), "Red Local Inalámbrica Para Empresas", **Revista de Telecomunicaciones de ALCATEL** (4): 287-91.

6. Riezenman, Michel J. (2002). "The ABCs of IEEE 802.11". **IEEE Spectrum** 39(9): 20.

7. Weatherspoon, Sultan. "Overview of IEEE 802.11b Security". **Network Communications Group**.

Disponible en: http://www.intel.com [consultado 11/02/2004]

ANEXO 1

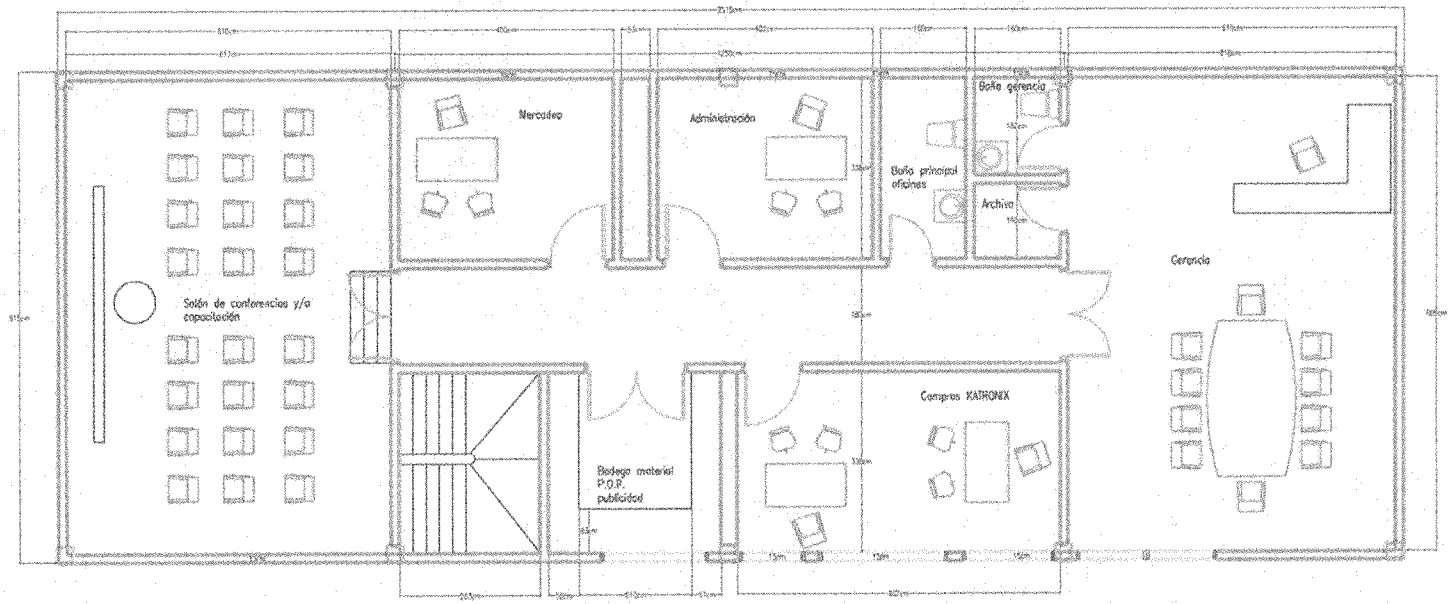
Después de realizar el levantamiento de información del punto de venta de Ktronix Calle 94, revisar la red que se tiene instalada, y las instalaciones Físicas decidimos ubicar 2 Routers Inalámbricos con antenas bidireccionales, que cubrirán el área de exhibición de computadores, notebooks, Imac y Palms.

El primer Router se encontrara ubicado a la entrada del Punto de venta, en este sitio no hay ningún tipo de interferencia ni paredes que dificulten la transmisión de la señal, lo que permitirá una comunicación estable entre los diferentes equipos de esta área.

El segundo Router se ubicara en el espacio destinado a la exhibición de PC's de Escritorio, Notebooks, Imac, en este sector no hay paredes o elementos que interfieran con la señal por la cual los equipos no tendrán ningún problema de conexión.

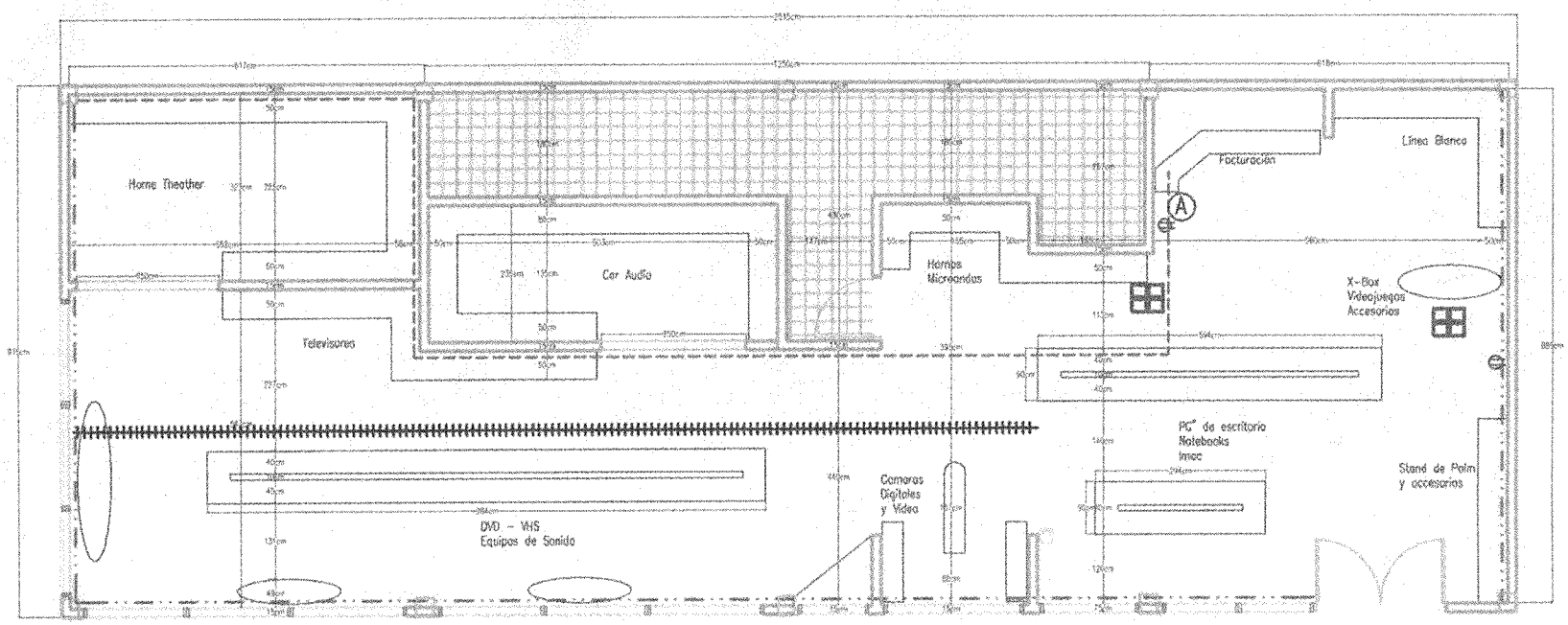
Los Routers estarán conectados a un AccesPoint el cual estará en conexión directa con la Red LAN del punto de venta, brindando asi conexión a Internet a todos los equipos cubiertos por los 2 hotspots.

PLANOMETRIA KTRONIX 94 PUNTO DE VENTA



ALKOSTO
LO DICE TODO
Compra Inteligente

K-TRONIX



K-TRONIX

ALKOSTO
LO DICE TODO
Compra Inteligente

PLANOMETRIA KTRONIX 94 PUNTO DE VENTA