UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE REDES INALÁMBRICAS USANDO TECNOLOGÍA WI-FI

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE :

INGENIERO ELECTRÓNICO

PRESENTADO POR :

ARTURO ENRIQUE CASTRO RAZURI

PROMOCIÓN
2000 - II

LIMA – PERÚ

2006

IMPLEMENTACIÓN DE REDES INALÁMBRICAS USANDO TECNOLOGÍA WI-FI

DEDICATORIA

Mi mayor gratitud a mis profesores y amigos
de la Facultad de Ingeniería Eléctrica y Electrónica
por aquellos inolvidables momentos compartiendo
múltiples experiencias y enseñanzas que conllevaron
a mi formación personal y profesional

SUMARIO

El presente informe de suficiencia tiene como objetivo presentar un modelo para la implementación de un red inalámbrica dentro de la Facultad de Ingeniería Eléctrica y Electrónica de la Universidad Nacional de Ingeniería (UNI), para tal motivo nuestro informe se ha dividido principalmente en tres capítulos

Marco teórico, en este capítulo se definen brevemente los conceptos teóricos de las tecnologías usadas actualmente en la implementación de redes inalámbricas, detallando sus ventajas, estándares, topologías, organismos reguladores, seguridad de información, etc.

Marco Legal, en este capítulo se definen las principales aspectos y normas legales a tener en cuenta en el diseño e implementación de nuestra red inalámbrica.

Aplicación, en este capítulo se detallan los parámetros necesarios para el diseño e implementación de nuestra red inalámbrica en distintos ambientes de la Facultad de Ingeniería Eléctrica y Electrónica de la UNI.

La intención de estos colectivos es crear a futuro una gran red, mediante la unión de pequeñas redes, libres e independientes.

Finalmente, presentamos las conclusiones obtenidas en la elaboración del presente informe.

ÍNDICE

INTRODUCCIÓN

La motivación principal para llevar a cabo este proyecto, ha sido poder realizar un estudio completo y objetivo de las principales tecnologías inalámbricas que existen actualmente, llegando a ser exhaustivo para la certificación Wi-Fi *(Wireless Fidelity)*, valorar su eficiencia, adaptación al medio, seguridad y costes, de tal forma que los investigadores y profesionales puedan realizar proyectos de implementación de redes inalámbricas con mayores garantías de éxito.

Este proyecto es una propuesta técnica para la implementación de una red de trabajo sin el uso de cables, conocida como WLAN *(Wireless Local Area Network)*, tomando como piloto distintos ambientes de la Facultad de Ingeniería Eléctrica y Electrónica de la Universidad Nacional de Ingeniería, haciendo uso de equipos con tecnología Wi-Fi con el objetivo de acceder a la red interna del campus universitario en forma inalámbrica.

En un principio la expresión Wi-Fi era utilizada únicamente para aparatos con una tecnología determinada, actualmente el desarrollo de las redes inalámbricas es de aceptación universal bajo estándares que operan en determinadas bandas de frecuencia y permiten la transmisión de información o datos a altas velocidades. Con el fin de evitar confusiones en la compatibilidad de los equipos y la interoperabilidad de las redes el término Wi-Fi se extendió hacia aparatos de distintas tecnologías.

CAPÍTULO I
MARCO TEÓRICO

El objetivo de este capítulo es definir los conceptos teóricos y técnicos de las distintas tecnologías y estándares que usaremos en el diseño e implementación de nuestra red inalámbrica, enfocando principalmente las ventajas, los modos de operación y la seguridad de información que nos brinda en la actualidad la tecnología Wi-Fi.

1.1 Redes Inalámbricas

Una red WLAN o Red de Area Local Inalámbrica, es un sistema de comunicación de datos flexible que se incorpora como una extensión o una alternativa a la red LAN con cable. Utilizan ondas de radio de alta frecuencia en lugar de cables para la transmisión y recepción de datos, minimizando la necesidad de conexiones con cable, de esta forma las redes inalámbricas combinan la conectividad de datos con la movilidad del usuario.

En una configuración WLAN habitual un dispositivo transmisor / receptor, denominado Punto de Acceso *(Access Point)*, brinda cobertura de red desde una ubicación fija a equipos portátiles o fijos equipados denominados Clientes *(Host)* usando tarjetas de red inalámbricas, proporcionando un ancho de banda máximo compartido.

1.1.1 Elementos de una Red Inalámbrica

Punto de Acceso Wireless (PA)

Es el dispositivo inalámbrico central de una WLAN que mediante un sistema de radio frecuencia (RF) se encarga de recibir y enviar información de diferentes estaciones móviles para su centralización y enrutamiento.

Es el punto de interconexión de una red inalámbrica con una red de cable, podemos disponer de diferentes puntos de acceso en una misma red, configurándolos individualmente como subredes o para permitir el desplazamiento físico de uno a otro sin perder la conexión, este dispositivo funciona a modo de repetidor de señal, distribuyendo la información entre los distintos destinos finales. Para mayor detalle ver Cap. III [6].

En la Fig. 1.1 se muestran algunos modelos de puntos de acceso para redes inalámbricas.

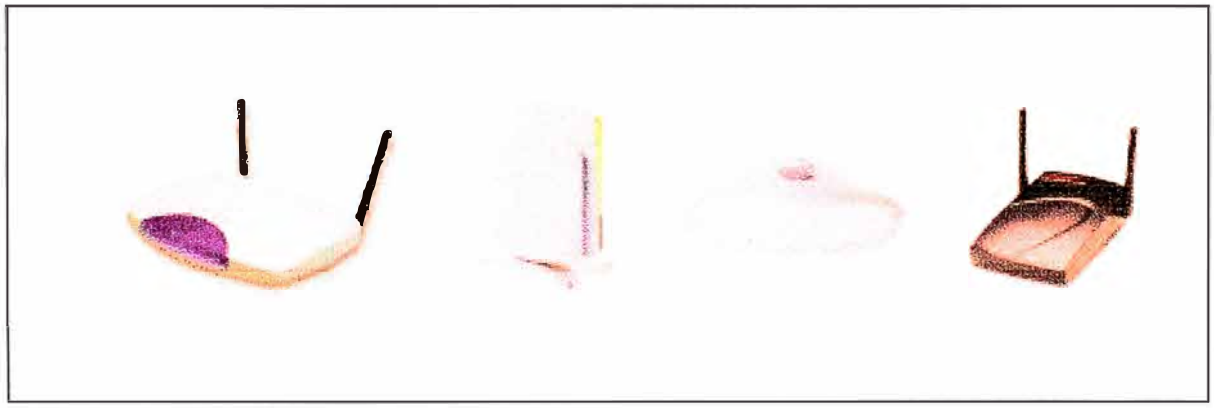

Fig. 1.1 Puntos de Acceso Inalámbricos

Estaciones o Clientes

Dispositivos finales que acceden a los puntos de acceso (PA) a través de tarjetas inalámbricas de acceso. Las estaciones o equipos clientes son los terminales de los usuarios de red, pueden ser ordenadores fijos portátiles, terminales de mano, PDA's, etc.

Adaptadores o tarjetas de red inalámbricas

Se refieren a las tarjetas típicas de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Generalmente este hardware es del tipo PCMCIA ya que su tamaño y facilidad de conexión lo hace mas apropiado para equipos portátiles, no obstante también existen versiones para otro tipo de conectores tales como USB, PCI o ISA (para ordenadores de sobremesa) y en formato SD (para PDA's, Palm, etc.), esto nos permite conectar los dispositivos a cualquier tipo de ordenador. Para mayor detalle ver Cap. IV [6]

En la Fig. 1.2 se muestran algunos modelos de adaptadores usados en la implementación de redes inalámbricas.

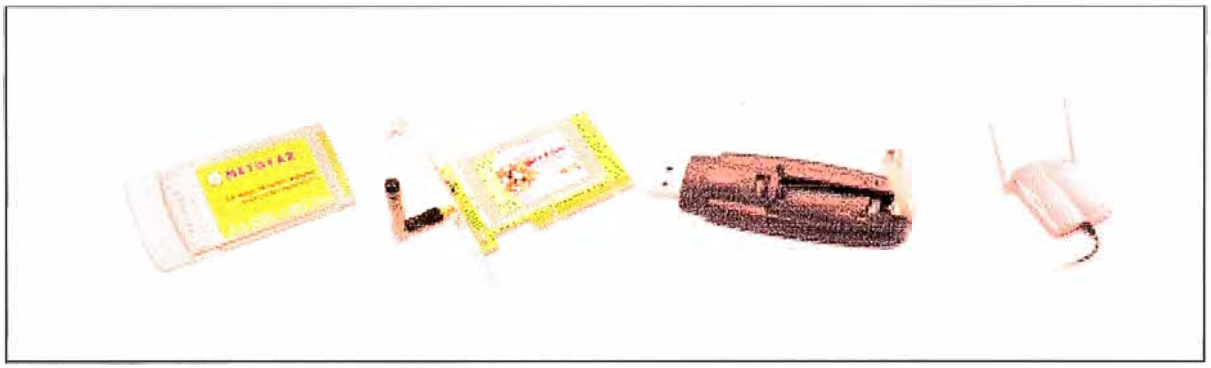

Fig. 1.2 Adaptadores para redes inalámbricas.

Antenas de repetición de señal

Son dispositivos generalmente metálicos capaces de radiar y recibir ondas de radio que adaptan la entrada/salida del receptor/transmisor del medio. Son necesarios para conseguir una señal uniforme en puntos alejados. Existen dos tipos de antenas generalmente usadas en redes inalámbricas

Omnidireccionales :

Estas antenas actúan a modo de bombilla retransmitiendo la señal en todas las direcciones.

Direccionales :

Actúan a modo de foco, retransmitiendo la señal en una sola dirección pero con mayor potencia. Para mayor detalle ver Cap. I [3].

1.1.2 Características de las Redes Inalámbricas

- En este tipo de redes se usan bandas de frecuencia de libre uso, es decir bandas no licenciadas.

- La seguridad es una de las mayores tareas pendientes, a la espera de estándares que garanticen las transmisiones inalámbricas seguras.

La cobertura de la red dependerá de la tecnología usada en el diseño e implementación.

Los estándares más usados en este tipo de redes son de tecnología 802.11a, 802.11b y 802.11g .

La Tabla 1.1 nos muestra las características más importantes de dichos estándares.

1.1.3 Ventajas

Utilizando una WLAN se puede acceder a información compartida sin necesidad de buscar un lugar para conectar el computador, y los administradores de la red pueden poner a punto o aumentar la red sin necesidad de instalar o mover cables. Como una visión general de los beneficios de una WLAN frente a las redes tradicionales, debido al avance de la tecnología y la eliminación del uso de cables podemos mencionar las siguientes ventajas en cuanto a productividad, comodidad y costos:

Estandarización e Interoperabilidad, nos permite obtener compatibilidad entre los equipos y estándares usados.

- **Movilidad,** nos brinda información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red, el que se obtenga en tiempo real supone mayor productividad y posibilidad de servicio. Permite la conexión desde cualquier punto dentro de cobertura, incluso en movimiento.

Ahorro de costes, cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación. Se obtiene una significativa reducción del presupuesto en comparación a las redes con cableados fijos y líneas dedicadas.

Acceso temporal, se puede obtener conexión temporal desde lugares de emergencia, congresos, edificios, residencias, empresas, etc.

Facilidad de instalación, nos brinda simplicidad y rapidez en la instalación, mejor gestión y ahorro de espacio, evita realizar obras para tirar cable por muros y techos.

- **Flexibilidad,** permite el acceso a una red en entornos de difícil cableado.

  Adaptabilidad, permite frecuentes cambios de la topología de la red y facilita su escalabilidad.

1.1.4 Inconvenientes

Sin duda son múltiples las ventajas y avances logrados hasta la actualidad, sin embargo aún existen inconvenientes que debemos tener en cuenta. Entre las deficiencias de la redes inalámbricas que se encuentran en proceso de evolución podemos mencionar las siguientes

Seguridad, aunque existen soluciones, esta es una de las mayores tareas pendientes, a la espera de estándares que garanticen mayor seguridad a las transmisiones inalámbricas.

Consumo eléctrico, debido al uso de equipos y aparatos de última generación el consumo de energía hacia estos dispositivos es relativamente alto, se espera que a corto plazo tienda a disminuir.

1.1.5 Estándares Existentes

El comité IEEE 802.11 es el encargado de desarrollar los estándares para las redes de área local inalámbricas.

El estándar IEEE 802.11 se basa en el mismo marco de estándares que Ethernet, esto nos garantiza un excelente nivel de interoperatividad y asegura una implementación sencilla de las funciones y dispositivos de la interconexión Ethernet/WLAN.

A continuación presentaremos en forma detallada las principales características de los estándares inalámbricos existentes

Estándar 802.11 (Estándar original)

- Presenta un ancho de banda máximo de hasta 2 Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencias.
- Presenta posibles interferencias con hornos microondas, dispositivos bluetooth y teléfonos DECT, puesto que operan en el mismo espectro de frecuencias.
- Utiliza los sistemas de modulación FHSS *(Espectro Distribuido con Saltos de Frecuencias)* y DSSS *(Espectro Ensanchado de Secuencia Directa)*.

Estándar 802.11a (54 Mbps, 5 GHz)

- Presenta un ancho de banda máximo de hasta 54 Mbps.
- Opera en el espectro de 5 Ghz sin necesidad de licencia, menos saturado.
- No es compatible con los estándares 802.11b y 802.11g.
- Usa el sistemas de modulación OFDM *(Multiplexación por división de frecuencia ortogonal)*.

Estándar 802.11b (11Mbps, 2.4 GHz)

- Es el estándar predominante en redes locales para la empresa y el hogar, así como puntos de conexión públicos.
- Presenta un ancho de banda máximo de hasta 11 Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Presentan las mismas interferencias que el estándar 802.11.
- Este estándar también es conocido como Wi-Fi.
- Utiliza el sistema de modulación DSSS.
- Es compatible con los equipos DSSS del estándar 802.11.

Estándar 802.11g (54 Mbps, 2.4 GHz)

- Presenta un ancho de banda de hasta 54 Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Es compatible con el estándar 802.11b.
- Usa sistemas de modulación DSSS y OFDM .

Tabla 1.1. Estándares más usados en redes inalámbricas

	802.11b	**802.11g**	**802.11a**
Banda	2.4 Ghz	2.4 Ghz	5 Ghz
Velocidad	1 – 11 Mbps	24 - 54 Mbps	20 - 54 Mbps
Número de canales no solapados	3	3	8
Wi-Fi	Si	Si	Si
IEEE	1999	2003	1999

La Tabla 1.1 nos presenta algunos datos comparativos de los tres estándares más usados en redes inalámbricas, aquí se detallan el ancho de banda, la velocidad y el número de canales de operación. Para mayor detalle ver Cap. VII [3].

Extensiones de los estándares inalámbricos :

Estándar 802.11d - Dominios adicionales de regulación.

Constituye un complemento de control de acceso al medio (MAC) en el estándar 802.11, para proporcionar el uso a escala mundial de las redes WLAN, permitirá a los puntos de acceso comunicar la información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

Estándar 802.11e - QoS *(Quality of Service)*.

Su objetivo es proporcionar soporte de calidad de servicio (QoS) para aplicaciones de redes LAN. Se aplicará a los estándares fijos a, b y g de 802.11, la finalidad es proporcionar claves de servicios con niveles gestionados de QoS para aplicaciones de datos, voz y video.

La calidad de servicio (QoS), es el rendimiento de extremo a extremo de la comunicación, tal como lo percibe el usuario final. Los parámetros de la QoS son : El retardo, la variación del retardo y la pérdida de información. Una red debe garantizar un cierto nivel de calidad de servicio para un determinado nivel de tráfico.

La implementación de las políticas de QoS se pueden enfocar en varios puntos según los requerimientos de la red, los principales son

Asignar un ancho de banda en forma diferenciada.
Evitar y/o administrar la congestión de la red.
Manejar prioridades de acuerdo al tipo de tráfico.
Modelar el tráfico de la red.

Estándar 802.11f - IAPP *(Inter-Access Point Protocol)*.

Su objetivo es lograr la interoperabilidad de los Puntos de Acceso (AP) dentro de una red WLAN multiproveedor. El estándar define el registro y el intercambio de información entre dichos puntos de acceso cuando un usuario se traslada de un punto a otro.

Estándar 802.11i - Seguridad y Autenticación

Se refiere al objetivo mas frecuente del estándar 802.11, la seguridad. Se aplicará a los estándares fijos a, b y g. Proporciona una alternativa a la WEP *(Wired Equivalent Privacy)*, con nuevos métodos de encriptación y procedimientos de autentificación. Para mayor detalle ver Cap. VIII [6].

Estándar 802.11h - Mecanismos de selección dinámica de frecuencias y control de potencia de transmisión.

El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 Ghz. Estos reglamentos requieren que los productos tendrán control de la potencia de transmisión (TCP) y selección de frecuencia dinámica (DFS).

El control TCP limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. La DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas, en particular el radar.

1.2 Topología de una Red Inalámbrica

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas, para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y Ad-hoc. En este informe se utilizarán los términos "Infraestructura" y "Ad-hoc", estos términos están relacionados con las mismas distinciones básicas de topología.

Es conveniente hacer una división entre la topología y el modo de funcionamiento de los dispositivos Wi-Fi. Con topología nos referimos a la disposición lógica de los dispositivos, aunque la disposición física también se pueda ver influida, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida. Para mayor detalle ver Cap. VII [3].

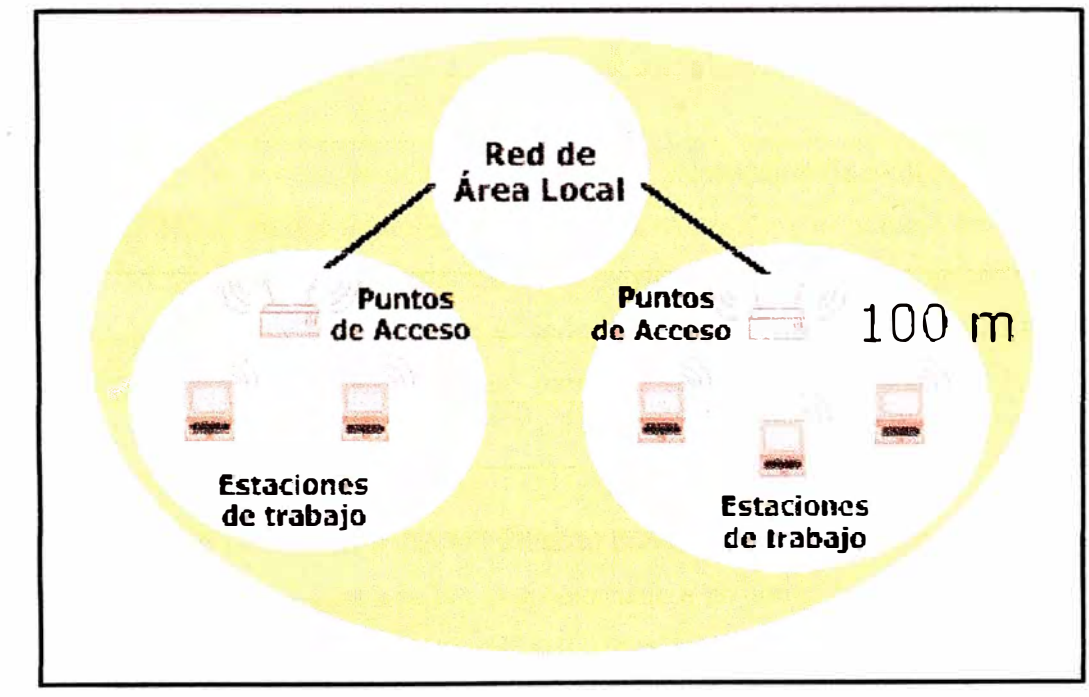

Fig. 1.3. Red LAN conectada a 2 redes WLAN

La Fig. 1.3 nos muestra una red LAN Ethernet conectada a 2 redes LAN inalámbricas (WLAN), usando dos puntos de acceso, los cuales brindan una cobertura de aproximadamente 100 metros de distancia a las estaciones de trabajo o estaciones cliente.

1.3 Modos de Operación

En el mundo wireless existen dos topologías básicas:

La topología Infraestructura y la topología Ad-hoc.

1.3.1 Topología Infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso, tal como se muestra en la Fig. 1.4. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y 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 específica; la extensión y el número de dispositivos dependen del producto y del estándar de conexión inalámbrica que se utilice. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

La Fig. 1.4 nos muestra una red Ethernet conectada a una red inalámbrica a través de un punto de acceso, el cual a su vez esta conectado a un punto de extensión para brindar una mayor cobertura a los dispositivos finales, conformando de esta manera una red en modo infraestructura.

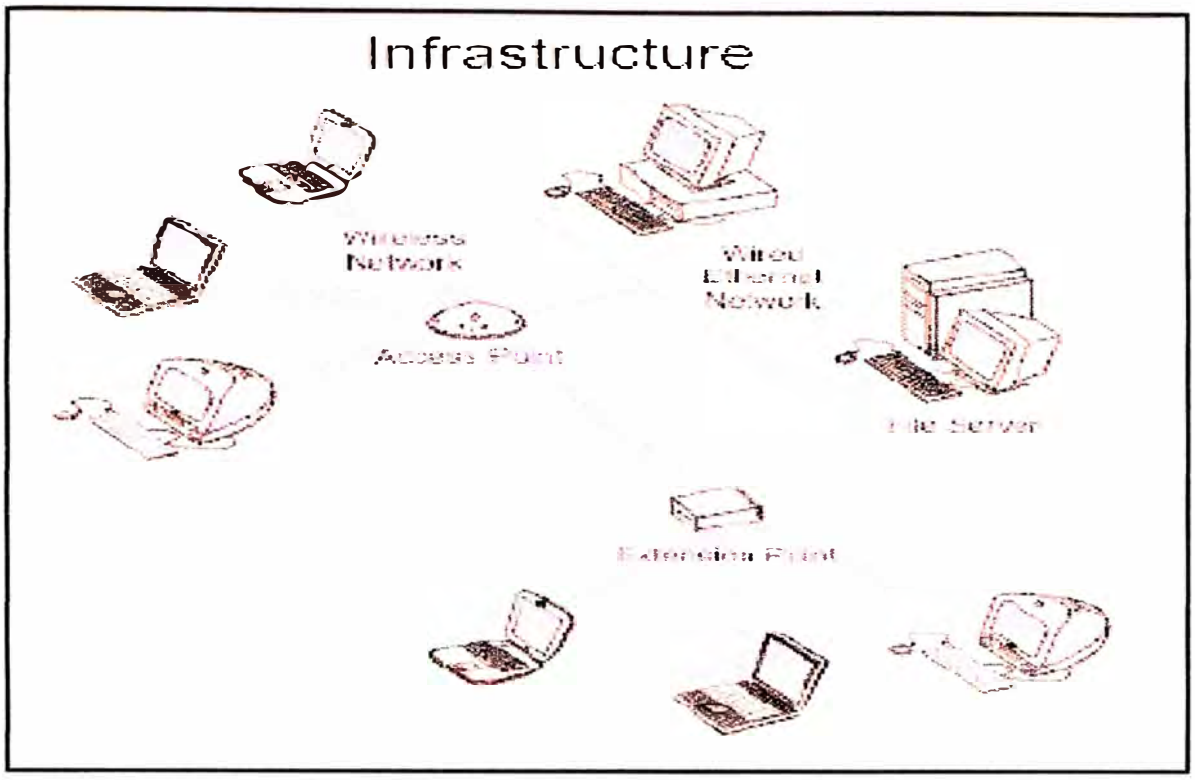

Fig. 1.4. Red en la modalidad de Infraestructura

1.3.2 Topología Ad-Hoc

En una topología Ad-hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso, tal como se muestra en la Fig 1.5.

Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas Ad-hoc podrían ser un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas. Para mayor detalle ver Cap. IV [4].

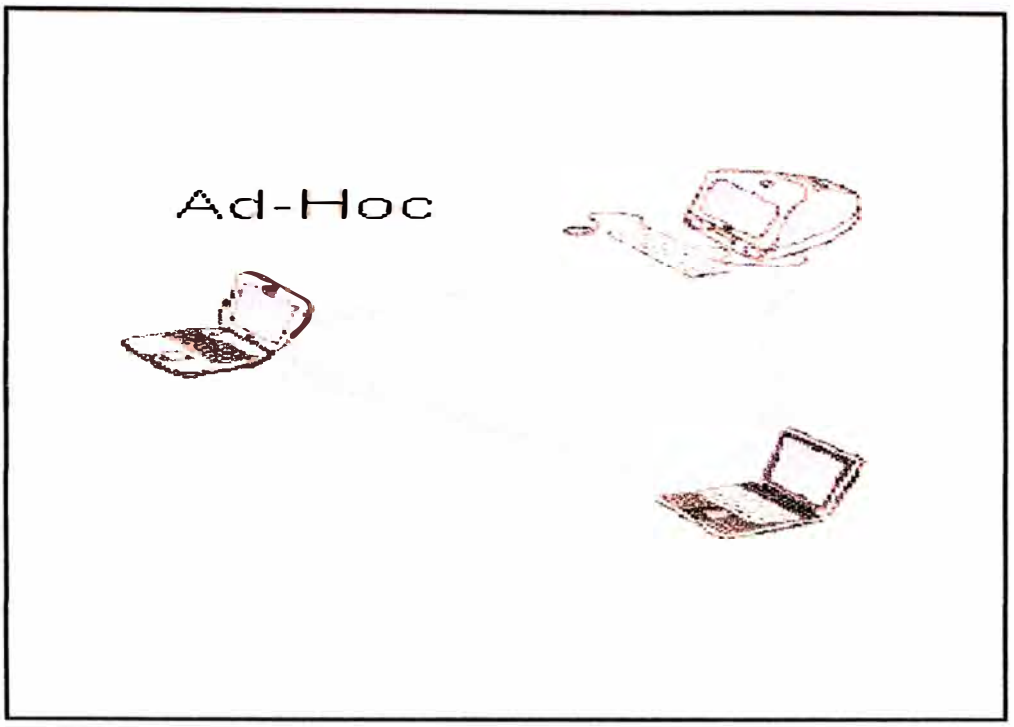

Fig. 1.5. Red en la modalidad Ad-Hoc

1.4 Pronóstico de Instalaciones Hot Spot en el Mundo

El Hot Spot es un punto de acceso generalmente localizado en lugares con gran tráfico de público que proporciona servicios de red inalámbrica de banda ancha a visitantes móviles . Para mayor detalle ver Cap. VII [3].

La Fig. 1.6 nos muestra la proyección de crecimiento de las instalaciones Hot Spot hacia el año 2006 en el mundo.

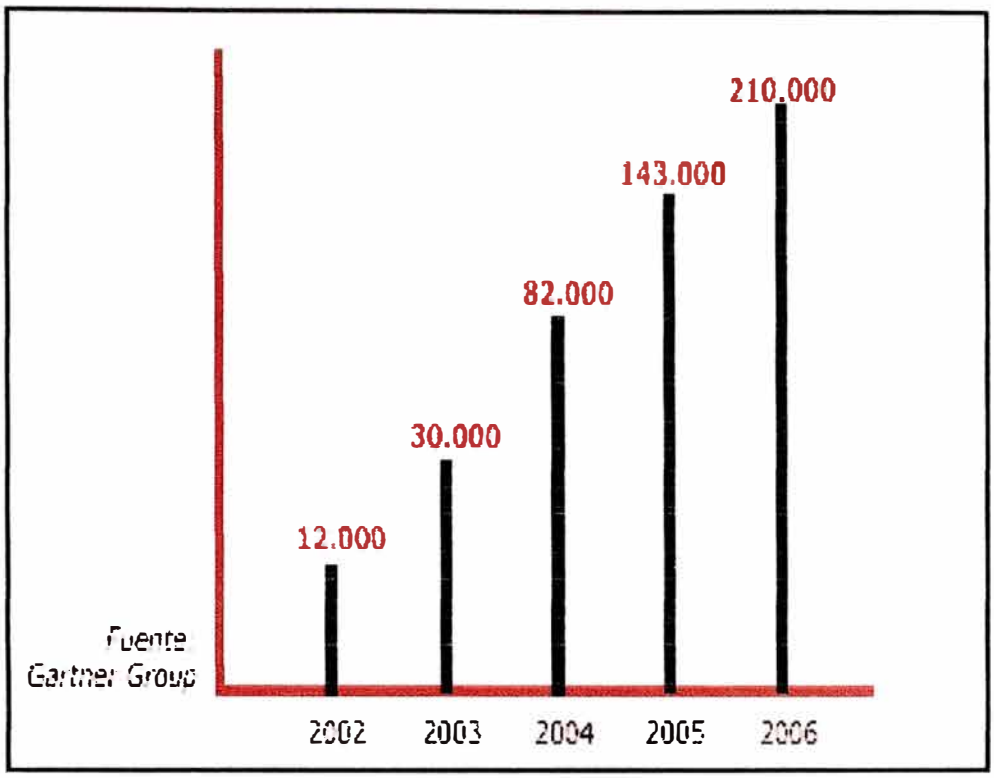

Fig. 1.6. Proyección de instalaciones Hot-Spot en el mundo

1.5 Redes Inalámbricas en la actualidad

La aparición en el mercado de las redes inalámbricas han introducido un nuevo lenguaje a la hora de hablar de redes de datos. Poder identificar correctamente la gran cantidad de nuevas siglas y acrónimos, esto es una ventaja importante a la hora de discutir una propuesta concreta. Por tal motivo, presentaremos los conceptos más importantes que se utilizan en este informe, así como un resumen del estado en que se encuentra esta tecnología en la actualidad.

Actualmente existen tres estándares de redes inalámbricas Wi-Fi, estos estándares determinan los detalles físicos de transmisión y recepción, como la velocidad de los datos, la banda de radio donde operan y las potencias máximas de emisión.

- Estándar 802.11b: Hasta 11 Mbps sobre la banda de 2,4 Ghz.
- Estándar 802.11g: Hasta 54 Mbps sobre la banda de 2,4 Ghz.
- Estándar 802.11a: Hasta 54 Mbps sobre la banda de 5 Ghz.

Estos estándares han sido aprobados para su uso, con el detalle de que para redes 802.11a los equipos que se instalen han de funcionar en modo de grupo de trabajo para interiores *(Workgroup)*, y no han de sobrepasar la potencia de emisión de 1 Vatio.

1.6 Seguridad en Redes Inalámbricas.

Para mantener la seguridad en una red inalámbrica se debe tener en cuenta lo siguiente:

- Cualquiera dentro de un radio de 100 metros puede ser un intruso potencial.
- Las acreditaciones del usuario se deben poder intercambiar con seguridad.
- Debe ser capaz de asegurar la conexión con la red de trabajo correcta.
- Los datos se deben poder transmitir con seguridad a través de la utilización apropiada de llaves de encriptación.

1.6.1 Seguridad WEP *(Wired Equivalent Privacy)*.

En redes Wi-Fi el concepto de la seguridad se extiende más allá de lo que representaba en redes cableadas. El hecho de poder acceder al tráfico de una red sensible sin ser necesaria una presencia física, obliga a extremar las medidas de seguridad en entornos corporativos.

Por ello, el primer estándar Wi-Fi (802.11b) incorpora desde su origen un sistema de seguridad denominado WEP, basado en la encriptación de la información.

De todas formas, la popularización de las redes Wi-Fi puso de manifiesto ya en sus inicios que WEP presentaba una serie de vulnerabilidades, debido principalmente al uso de claves estáticas de pocos bits y a un sistema de autenticación débil, que lo hacían poco útil para redes corporativas.

Para contrarrestar estos problemas aparecieron en el mercado soluciones basadas en dos enfoques complementarios:

- Autenticación 802.1x con claves dinámicas más largas.
- Redes privadas virtuales entre los clientes inalámbricos y la red local.

Características de la Seguridad WEP

- Sistema de encriptación estándar 802.11.
- Se implementa en la capa de Control de Acceso al Medio (MAC) .
- Soportada por la mayoría de vendedores de soluciones inalámbricas.
- Cifra los datos enviados a través de las ondas de radio.
- Utiliza algoritmos de encriptación.

1.6.2 Seguridad WPA *(Wi-Fi Protected Access)*

Si bien la utilización de estas alternativas proporcionaban una primera solución al problema de la seguridad en las redes inalámbricas, también presentaban una serie de desventajas que las hacían poco viables, tales como:

- Desarrollos propietarios.
- Nivel de seguridad limitado intrínsicamente por la debilidad de WEP.
- Poca escalabilidad.

Para dar una respuesta final a este problema, el IEEE comenzó en 2002 a desarrollar un nuevo estándar de seguridad para redes Wi-Fi, denominado 802.11i, con el objetivo de que cumplieran todos los requisitos de seguridad necesarios para ser aplicable tanto en entornos corporativos como en entornos PYME y domésticos.

El hecho de que 802.11i no estuviera disponible hasta bien entrado el 2004, unido a la presión del mercado, hizo que la Wi-Fi Alliance se adelantara al IEEE promoviendo entre los principales fabricantes un estándar de-facto, nos estamos refiriendo al WPA, el cual quedó definido a principios de 2003. Este estándar cumple una serie de requisitos básicos:

- Es compatible con el estándar 802.11i
  Seguridad fuerte para entornos corporativos y pequeños
  Disponible para la actualización de software en los equipos existentes
  El estándar WPA es mas fuerte que el estándar WEP
  Obligatorio a finales del 2003

A continuación, en la Tabla 1.2 se muestra un esquema comparativo de las principales características de los estándares de seguridad inalámbrica anteriormente comentados.

Tabla 1.2. Estándares de Seguridad Inalámbrica

	WEP	WPA	802.11 (RSN, WPA2)
Cipher Algorithm	RC4	RC4 (TKIP)	Rijndael (AES-CCMP)
Encryption Key	40-bit	128-bit (TKIP)	128-bit (CCMP)
Initialization Vector	24-bit	48-bit (TKIP)	48-bit (CCMP)
Authentication Key	None	64-bit (TKIP)	128-bit (CCMP)
Integrity Check	CRC-32	Michael (TKIP)	CCM
Key Distribution	Manual	802.1x (EAP)	802.1x (EAP)
Key unique to:	Network	Packet, session, user	Packet, session, user
Key hierarchy	No	Derived from 802.1x	Derived from 802.1x
Cipher Negotiation	No	Yes	Yes
Ad-hoc (P2P) security	No	No	Yes (IBSS)
Pre-authentication (wired LAN)	No	No	Using 802.1x (EAPOL)

Como se puede apreciar, el estándar WPA incorpora un nuevo sistema de encriptación (TKIP) y de autenticación y distribución de claves (802.1x). Desde septiembre de 2003, la mayoría de nuevos equipos Wi-Fi ya soportan este estándar. Para mayor detalle ver Cap. VIII [6].

Características de la Seguridad WPA :

- El estándar WPA es más fuerte que el WEP.
- Mejorable a través de nuevas versiones de software.
- Uso empresarial y casero.
- Obligatorio a finales del 2003.

1.6.3 Mejoras en la Seguridad de Redes Inalámbricas

Dentro de las mejoras que se han implementado a los estándares de seguridad inalámbrica podemos mencionar

- **TKIP** *(Temporal Key Integrity Protocol)*

Para el estándar 802.11, el cifrado de privacidad equivalente cableada (WEP) es opcional. Para WPA, se requiere el cifrado con el protocolo TKIP, este protocolo sustituye a WEP con un algoritmo nuevo de cifrado más seguro, sin embargo, utiliza las utilidades de cálculo de los dispositivos inalámbricos existentes para realizar las operaciones de cifrado.

Adicionalmente TKIP también nos proporciona :

- La comprobación de la configuración de seguridad después de determinar las claves de cifrado.
- El cambio sincronizado de la clave de cifrado para cada marco.
- La determinación de una clave de inicio de cifrado exclusiva para cada autenticación.

Autenticación de usuarios

Ofrece una autenticación fuerte mutua, tanto de la estación como del punto de acceso, brindando credenciales de seguridad y claves de encriptación dinámicas.

La Tabla 1.3 nos muestra una tabla comparativa de las funciones y características más relevantes de los estándares de seguridad WEP y WPA.

Tabla 1.3. Funciones de los Estándares WEP y WPA

Función	WEP	WPA
Encriptación	Débil	Soluciona debilidades
Claves	40 bits	128 bits
Claves	Estáticas	Dinámicas
Claves	Distribución manual	Automática
Autenticación	Débil	Fuerte, según 802.1x y EAP

1.6.4 Autenticación de Clientes de Red

Como hemos comentado, la autenticación en entornos WPA corporativos se basa en el estándar 802.1x, este estándar no define qué autenticación se utilizará, sino de que manera se realizará la negociación concreta de una autenticación determinada. Es el protocolo EAP *(Extensible Authentication Protocol)*, incluido en el estándar 802.1x, el que define el procedimiento para realizar esta negociación.

Esto permite que la autenticación en entornos WPA soporte varios métodos diferentes, cada uno con sus propias ventajas e inconvenientes. La clave al implementar el WPA en una red Wi-Fi, consiste en decidir el tipo de autenticación que se utilizará, ya que esto determinará los componentes necesarios para ponerla en marcha. Existe en la actualidad una multitud de métodos EAP especificados (alrededor de 40).

El hecho de que el EAP esté soportado en Windows XP e integrado con el servicio Wireless Zero Configuration y el servidor Radius de Windows, hace que parezca la solución más interesante a la hora de desplegar redes nuevas en entornos Microsoft que no dispongan de una infraestructura consolidada. De todas maneras, esto no es generalizable, y se debe contemplar en cada caso la mejor solución.

Para redes pequeñas y/o domésticas, el estándar WPA también contempla un modo de funcionamiento especial (WPA-PSK), que permite evitar la utilización de un servidor Radius y del protocolo 802.1x-EAP correspondiente. Este modo utiliza claves preasignadas *(pre-shared keys)* localmente en los puntos de acceso y en los clientes de red para realizar la autenticación.

Una vez realizada, la encriptación y el cambio dinámico de claves se efectúan de la misma manera anteriormente comentada (vía TKIP), lo que permite obtener un nivel de seguridad muy superior al conseguido vía WEP, a su vez que la dificultad en la implementación resulta ser mínima. Para mayor detalle ver Cap. VII [3].

Autenticación 802.1x

La autenticación 802.1x presenta las siguientes características

- Provee un método para la autenticación y autorización de conexiones a una red inalámbrica.
- La autenticación es basada en el usuario; se puede usar credenciales tales como contraseñas o certificados.
- Utiliza el protocolo de autenticación extensible (EAP) entre la estación móvil y el punto de acceso.
- Aprovechamiento de protocolos AAA tales como Radius para centralizar la autenticación y las autorizaciones.

Servidor Radius *(Remote Authentication Dial In User Service)*

El Servidor Radius presenta las siguientes características :

- La autenticación se basa en el usuario, en vez de basarse en el dispositivo.
- Elimina la necesidad de almacenar información de los usuarios en cada punto de acceso de la red, por tanto es considerablemente más fácil de administrar y configurar.
- Radius ha sido ampliamente difundido para otros tipos de autenticación en las redes de trabajo.

Protocolo de Autenticación Extensible (EAP)

El EAP es una extensión del Protocolo Punto a Punto (PPP), proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros.

Junto con los métodos de autenticación EAP de alto nivel es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, a diferencia de otros métodos de autenticación.

Una VPN es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. La idea es que la red pública sea vista desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

Las Virtual Private Networks (VPN) son una alternativa a la conexión WAN mediante líneas telefónicas, bajando los costos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones. Los tipos de autenticación EAP proveen de seguridad a las redes 802.1x

- Protegen las credenciales.
- Protegen la seguridad de los datos.

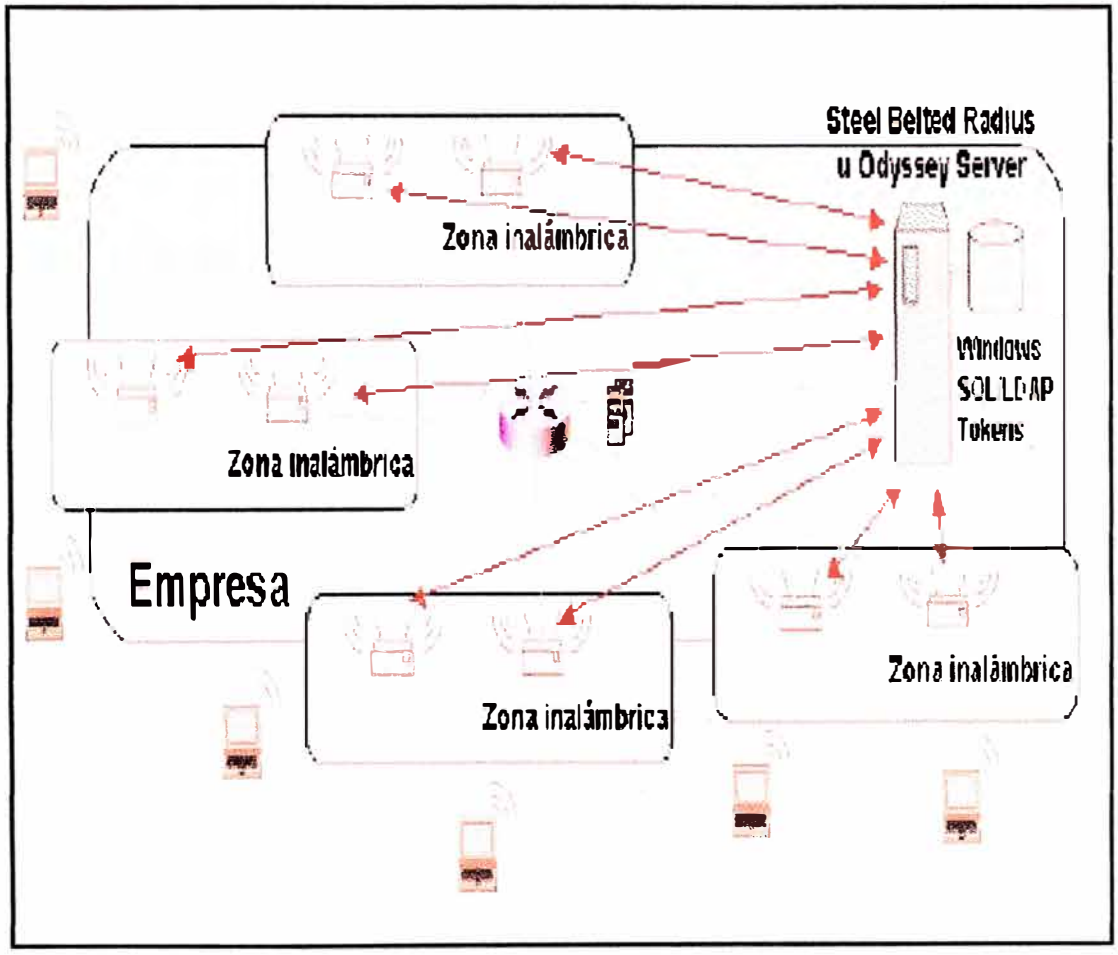

Fig. 1.7 Red Inalámbrica en una Empresa, la solución según 802.1x

En la Fig. 1.7 se aprecia la red inalámbrica de una empresa, cuyo sistema de seguridad esta basado en autenticación 802.1x-EAP, administrada y centralizada por un servidor Radius.

WarChalking

Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

En la Fig. 1.8 se aprecia a un individuo o hacker potencial tratando de conectarse a la red inalámbrica de una institución usando una PC y un adaptador inalámbrico desde su auto.

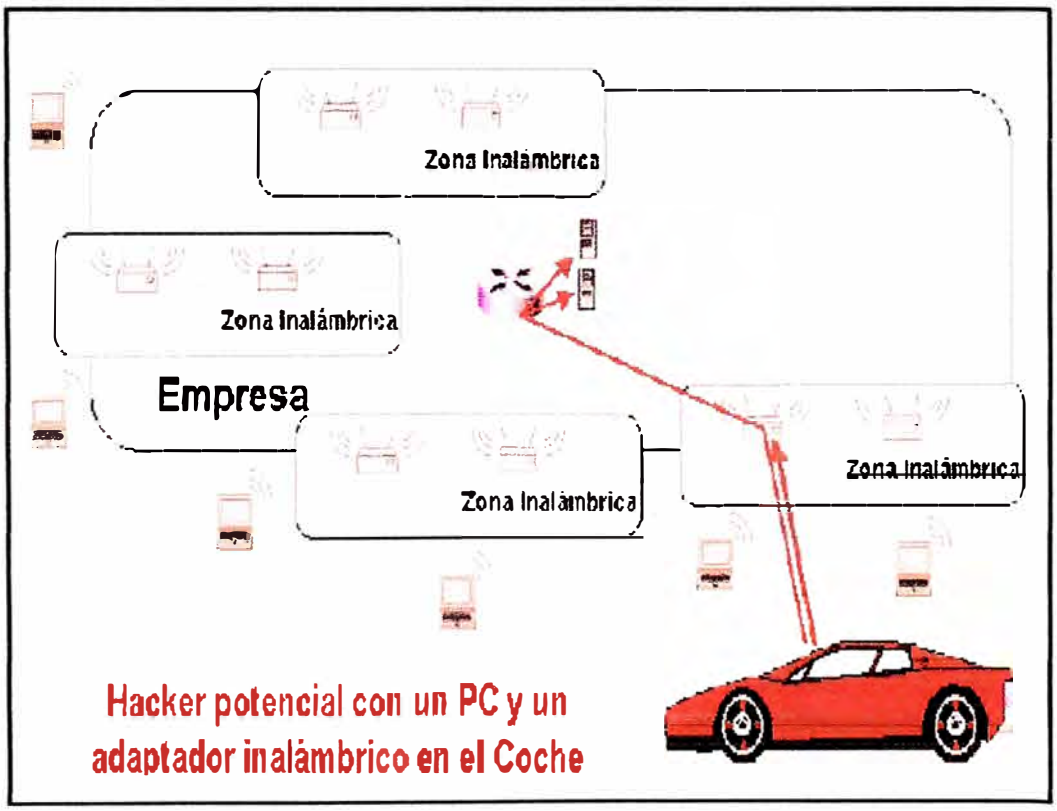

Fig. 1.8 Red Inalámbrica en una Institución, Ataque Potencial 1

WarDriving

Es una técnica difundida donde individuos equipados con material apropiado tratan de localizar desde un auto puntos inalámbricos.

En la Fig. 1.9 se aprecia a un individuo tratando de conectarse a la misma red haciendo uso de un punto de acceso ubicado en el interior del auto, el cual intentará conectarse a los dispositivos finales y posteriormente al servidor de la red. Para mayor detalle ver [11].

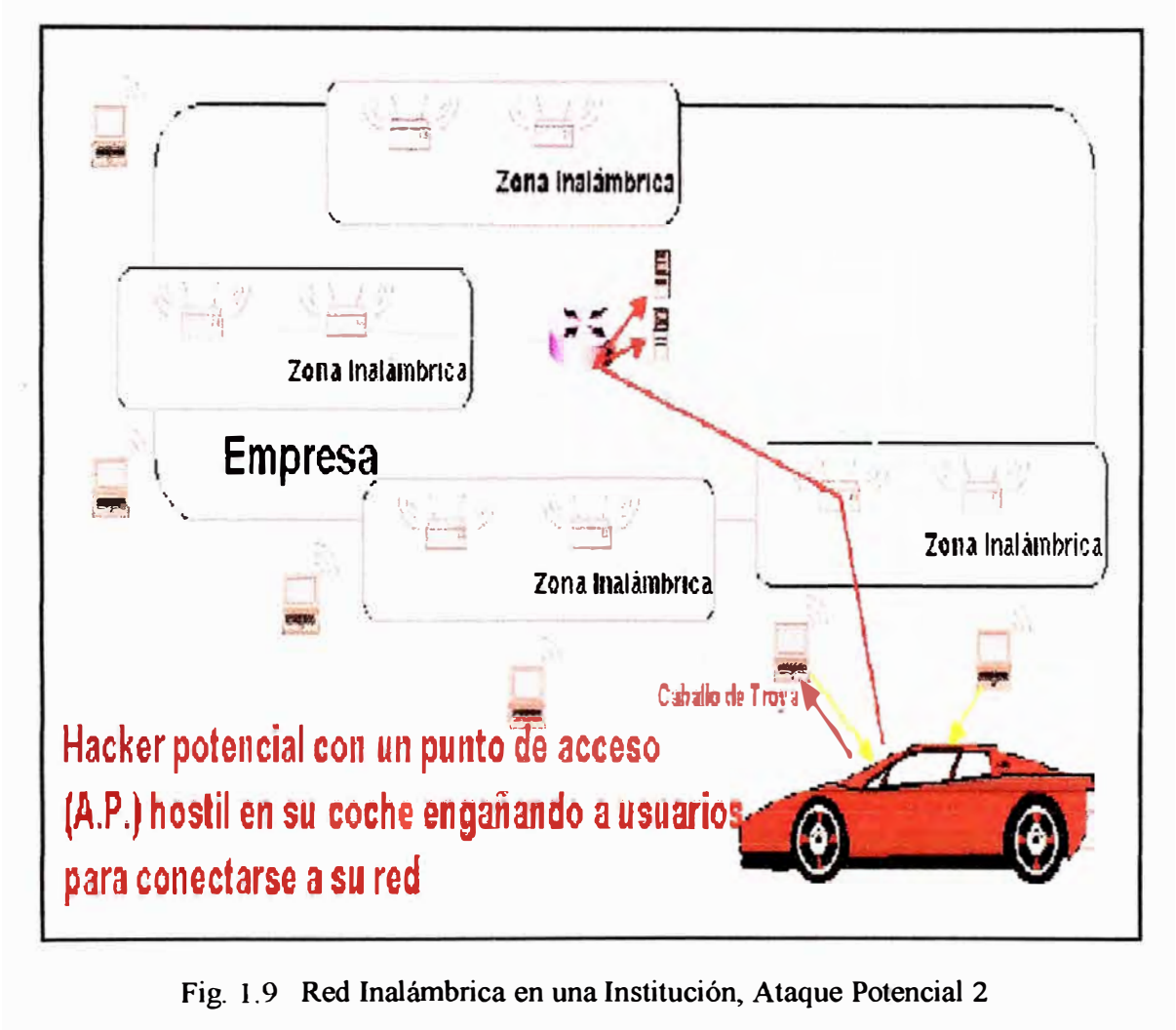

Fig. 1.9 Red Inalámbrica en una Institución, Ataque Potencial 2

1.7 Tecnología WI-FI

Es un conjunto de normativas referentes a la interconexión de sistemas inalámbricos mediante tecnología de radio. Este sistema en su aspecto de recepción de radio es equivalente en potencia y características a los mandos a distancia de las puertas de garaje, los teléfonos inalámbricos domésticos o los mandos a distancia de los automóviles.

La expresión Wi-Fi, abreviatura de Wireless Fidelity, se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin el uso de cables, funcionando con todo tipo de sistemas operativos, tales como : Linux, Windows, Solaris, Unix, etc. Para mayor detalle ver Cap. I [6].

Ventajas del sistema WI-FI

Como una visión general de los beneficios que nos ofrecen los sistemas Wi-Fi frente a otros tipos de redes, debido al avance de la tecnología y la eliminación del uso de cables podemos citar las siguientes ventajas

Ahorro considerable de costes a la hora de instalar entornos LAN, siendo necesaria una infraestructura mínima, frente a la complicación, dificultad y alto coste para instalar redes Ethernet, debiéndose adquirir cables y realizar obras de infraestructura.

Estas redes nos brindan largo alcance, hasta 3 ó 4 plantas de un inmueble, frente a una red convencional Ethernet, la cual necesita repetidores para cada planta.

- Fácil reposición ante incidencias no previstas.

- Al ser un sistema multiplataforma, facilita la portabilidad a otras aplicaciones en diferentes entornos, así como la migración a diferentes sistemas operativos. Para mayor detalle ver Cap. III [6].

1.7.2 Características de los estándares Wi-Fi

Dentro de las principales características técnicas de los estándares Wi-Fi usados en la implementación de redes inalámbricas podemos mencionar la frecuencia de operación, la tecnología, los tipos de modulación, el ancho de banda, los protocolos de acceso y la cobertura de red.

A continuación detallaremos dichas características para cada uno de los estándares Wi-Fi usados en la actualidad

Estándar 802.11b (Wi-Fi)

Frecuencia

Opera en la banda de 2.400 - 2.4835 GHz.
Esta banda también es conocida como ISM Band *(Industry, Science, and Medicine)*.

Tecnología

DSSS *(Direct Sequenced Spread Spectrum)*.

Modulación

CCK *(Complementary Code Keying)* - 5.5 Mbps / 11 Mbps
QPSK *(Quadraphase-shift Keying)* - 2 Mbps
BPSK *(Binary Phase Shift Keying)* - 1 Mbps.

Ancho de Banda

11 Mbps para la transmisión / ~ 5.5 Mbps efectivos
Fall back 5.5, 2 y 1 Mbps

Seguridad

WEP 64 bit, 128 bit de encriptación
SSID *(Service Set Identifier)*
Usa 802.1x y filtrado por MAC

Media Access Protocol

CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*

Distancia

Hasta 100 metros
Aprobado en Julio 1999

Estándar 802.11a (Wi-Fi)

Frecuencia

Opera en la banda de 5 GHz.
Conocida también como UNII Band *(Unlicensed National Information Infrastructure)*

Tecnología

OFDM *(Orthogonal Frequency Division Multiplexing)*

Modulación

64-QAM *(64-level quadrature amplitude modulated)* - 48/54 Mbps
16-QAM *(16-level quadrature amplitude modulated)* - 24/36 Mbps
QPSK - 12/18 Mbps

BPSK - 6/ 9 Mbps

Ancho de Banda

54 Mbps para la transmisión / ~ 30 Mbps efectivos
Fall back de 48, 36, 24, 18, 12, 9, 6 Mbps.

Seguridad

WPA
WEP 64 bit, 128 bit de encriptación
SSID
Autenticación 802.1x
Filtrado por MAC.

Media Access Protocol

CSMA/CA

Distancia

Hasta 100 metros
Aprobación Julio 1999

Estándar 802.11g (Wi-Fi)

Frecuencia

Opera en la banda de 2.412 - 2.4835 GHz
Conocida como ISM Band

Tecnología

DSSS
OFDM

Modulación DSSS

CCK - 5.5 / 11 Mbps

QPSK - 2 Mbps

BPSK - 1 Mbps

Modulación OFDM

64-QAM - 48/54 Mbps

16-QAM - 24/36 Mbps

QPSK - 12/18 Mbps

BPSK - 6/ 9 Mbps

Ancho de Banda

54 Mbps para la transmisión / ~30 Mbps efectivos.

Fall back 48, 36, 24, 18, 12, 9, 6 Mbps

Seguridad

WPA

WEP 64 bit, 128 bit de encriptación

SSID

Autenticación 802.1x

MAC Filtering.

Media Access Protocol

CSMA/CA

Distancia

Hasta 125 metros

Tabla 1.4 Características de los Estándares Wi-Fi

Estándar	802.11b	802.11a	802.11g
Velocidad	11 Mbps / 5.5 Mbps	54 Mbps / 30 Mbps	54 Mbps / 30 Mbps
Frecuencia	2.4 GHz	5.8 GHz	2.4 GHz
Precio	Económico	Alto	Accesible
Distancia máxima	50 – 100 m	50 –100 m	50 - 125
Popularidad	Amplia	Nuevo	Nuevo
Compatibilidad	Comunmente usado	No compatible	802.11b

En la Tabla 1.4 se muestra una tabla comparativa de las características mas importantes de los estándares Wi-Fi , tales como la velocidad, frecuencia, distancia, compatibilidad, etc. Para mayor detalle ver Cap. II [6].

1.8 Diseño de una red WLAN

El diseño de una WLAN esta referida a la conexión inalámbrica de cada punto destino con el punto de acceso mediante los adaptadores de cada equipo, con la posibilidad de conectar este a una red Ethernet ya existente. Además existe la posibilidad de conexión a la internet mediante diferentes tecnologías tales como ADSL *(Asymmetric Dynamic Subscriber Line)*, SDSL *(Symmetric Dynamic Subscriber Line)*, LMDS *(Local Multipoint Distribution System)*, Fibra Optica, etc. Para mayor detalle ver Cap. I-II [2].

1.8.1 Planeamiento y diseño de una red WLAN

Es muy común en este tipo de redes que los usuarios finales, entusiasmados por el boom que últimamente las WLAN's han alcanzado, compren e instalen equipos sin una previa planeación y diseño, trayendo como resultado un deficiente desempeño y en casos muy extremos, la pérdida de la información.

La instalación y la configuración de una WLAN pueden ser un proceso muy sencillo, pero precisamente esto las hace ser un blanco fácil para ataques externos e internos a la organización. Recordemos que el medio por el cual se comunican dispositivos inalámbricos es el aire, y que cualquier espía con los dispositivos necesarios puede rastrear las señales y utilizar en su beneficio los recursos de la red.

A continuación describiremos como planear y diseñar una red WLAN, con la intención de optimizar su desempeño así como también de reducir el nivel de inseguridad que presentan este tipo de redes.

Los factores que debemos tomar en consideración en el diseño y planeación de una red WLAN son

- Ancho de banda o velocidad de transmisión.
- Frecuencia de operación.
- Tipos de aplicaciones que van a correr en la WLAN.
- Número máximo de usuarios.
- Area de cobertura.
- Material con el que están construidos los edificios.
  Conexión de la WLAN con la red cableada.
- Disponibilidad de productos en el mercado.
- Planeación y administración de las direcciones IP.
- Los identificadores de la red (SSID).
  Seguridad.

Ancho de Banda / Velocidad de Transmisión

Debemos tomar en cuenta el ancho de banda y la velocidad de transmisión que nos brinda la WLAN. Los estándares IEEE 802.11a y IEEE 802.11g, permiten velocidades de hasta 54 Mbps, por otro lado el estándar IEEE 802.11b permite velocidades de transmisión de hasta 11 Mbps, este ancho de banda es mucho menor al de las redes cableadas, las cuales operan a 100 Mbps.

El ancho de banda especificado por los estándares 802.11a/b/g es teórico y se cumple sólo en condiciones ideales. El máximo desempeño depende de muchos otros factores.

Frecuencia de Operación

Cuando se diseña una WLAN generalmente causa confusión el hecho de seleccionar la frecuencia de operación que define el estándar que se va utilizar. Universalmente las WLAN's utilizan las frecuencias de 2.4 GHz (802.11b/g) y 5 GHz (802.11a).

Se han realizado diversos estudios sobre la propagación de las señales en estas dos frecuencias, dando como resultado que la frecuencia más baja (2.4 GHz) ofrece mejor propagación, extendiéndose más del doble de cobertura que la frecuencia de 5 GHz .

Tipos de aplicaciones

Es importante delimitar el tipo de aplicaciones que se van a correr en la red inalámbrica, tales como el acceso a Internet, correo electrónico, consultas a la base de datos y transferencia de archivos. Dado el limitado ancho de banda, no es recomendable que se utilicen las WLAN's para aplicaciones que consumen alto ancho de banda, tales como transferencia de video e imágenes, videoconferencia, audio y video.

Número máximo de usuarios

Uno de los factores más importantes cuando se diseña una WLAN es delimitar el número de usuarios que tendrán acceso a la red. Los estándares definen diferente número de usuarios conectados simultáneamente a un punto de acceso (AP). Es obvio afirmar que a mayor número de usuarios conectados a una WLAN, menor será el desempeño de la misma. Hay que tener en cuenta el número máximo de usuarios que soporta cada estándar.

Area de cobertura

Mientras la frecuencia aumenta, generalmente el rango de cobertura de la señal decrementa, de modo que la frecuencia de operación de 5 GHz generalmente tiene menor rango de cobertura que la de 2.4 GHz. De acuerdo con esto, si se utiliza el estándar 802.11a se requiere un número mayor de AP's para extender la cobertura, y esto implica un mayor presupuesto.

Por otro lado el estándar 802.11b tiene una mayor cobertura aunque con un menor ancho de banda. También hay que tener en cuenta si el punto de acceso se va a instalar en exteriores o interiores, ya que de ello dependerá el rango de cobertura. En cubículos cerrados la cobertura es de 20 metros, en cubículos abiertos de 30 metros, en pasillos o corredores es de hasta 45 metros y en exteriores de hasta 150 metros, el uso de antenas con mayor ganancia aumentará considerablemente la cobertura.

Material con el que están construidos los ambientes

La propagación de las ondas electromagnéticas (señales) se comportan de manera diferente en relación al material con el que estén construidos los edificios donde se instalará la WLAN. Hablamos entonces de diversos materiales tales como: madera, ladrillo, tabla roca. Ciertos materiales reflejan las señales sin problema como la madera y la tabla roca, lo cual puede extender la cobertura de la WLAN.

Otros materiales como el concreto con varilla, acero y cemento absorben o atenúan la potencia de la señal disminuyendo la cobertura.

Conexión de la WLAN con la red cableada

Debemos tener en cuenta que los puntos de acceso necesitan electricidad para poder operar y además deben estar conectados a la red cableada. Se recomienda instalar los puntos de acceso en lugares estratégicos sin olvidarse de éstas dos conexiones. Existen puntos de acceso que proveen la electricidad a través del cable par trenzado, esta característica se le conoce como PoE *(Power over Ethernet)*.

Disponibilidad de productos en el mercado

Debemos estar concientes del mercado de puntos de acceso. Si compramos un punto de acceso debemos de tomar en cuenta factores como el costo y el soporte técnico disponible. A veces lo barato puede salir caro.

Planeación y administración de las direcciones IP

Hay que tomar en cuenta que los dispositivos inalámbricos necesitan de una dirección IP para poder identificarse, por lo que será necesario reservar direcciones IP's para los dispositivos inalámbricos que se quieran conectar a la red. En caso de no existan las suficientes IP's, será necesario emplear enrutadores inalámbricos que puedan proporcionar direcciones IP privadas.

También hay que considerar el uso de servidores DHCP *(Dynamic Host Configuration Protocol)* para asignar direcciones dinámicamente, pero esto puede ser contraproducente. El servicio DHCP es un protocolo empleado para que los host (clientes) en una red puedan obtener una configuración a través de un servidor del protocolo, los datos así obtenidos pueden ser : La dirección IP, la máscara de red, la

dirección de broadcast, las características del DNS, etc. El servidor DHCP permite acelerar y facilitar la configuración de muchos clientes en una red, evitando en gran medida los posibles errores humanos. Finalmente el administrador de la red deberá decidir si se utiliza esta opción o asignar direcciones manualmente.

Los identificadores de la red (SSID)

Los SSID's son los identificadores de los puntos de acceso. Se deben poner los SSID's adecuados y no muy obvios debido a que los identificadores son fácilmente rastreables por diversas aplicaciones u otros AP's. Es muy común que al instalar un AP, no se cambie el nombre del SSID que trae de fábrica.

Esta mala práctica ocasiona que los usuarios maliciosos identifiquen claramente el nombre del fabricante del AP y puedan conocer la contraseña para finalmente entrar al panel de administración de la configuración del AP y tomar el control total de la red.

La Seguridad

La seguridad es quizás el factor menos tomado en cuenta al instalar una WLAN y resulta ser de lo más crítico. Las WLAN's son más susceptibles a ataques debido a que los intrusos no requieren conexión física para accesar a la red, en este punto hay que tener en cuenta cual será el nivel de seguridad que se requiere para proteger la red. Para mayor detalle ver Cap. VIII [6].

Fig. 1.10 Diseño de una Red Wi-Fi

En la Fig. 1.10 se muestra el diseño de una red Wi-Fi, usando un punto de acceso, el cual se encuentra conectado a una red cableada mediante un Router USB.

1.8.2 Garantía de instalación

Para comprobar que el sistema Wi-Fi puede cumplir con todos los requisitos ofertados en el entorno requerido, y con la finalidad de garantizar el correcto funcionamiento del servicio, se recomienda realizar una instalación previa a modo de prueba, donde se podrá comprobar que se cumplan con todos los requisitos especificados en los estándares IEEE 802.11b y 802.11g, bajo los que se rige el sistema Wi-Fi.

1.8.3 Presupuesto

Para poder realizar un presupuesto de la instalación de un sistema Wi-Fi en un área determinada es necesario conocer una serie de parámetros, que permitan realizar un diseño de red previo a la elaboración del presupuesto definitivo.

Estos parámetros son

- Número de plantas del inmueble.
- Altura del inmueble.
- Número de habitaciones de cada planta en la que se requiere poner la conexión.
- Diseño arquitectónico de cada planta.
- Material del que se componen las paredes.
- Posibilidad de introducir cableado adicional.
- Preferencias estéticas a la hora de implementar los componentes.
- Capacidad de la conexión a internet deseada para cada punto final.

1.9 Tecnologías Nuevas y Complementarias.

Dentro de las nuevas tendencias y las tecnologías complementarias a las redes Wi-Fi podemos destacar a los sistemas Wi-Max y Bluethoot.

Wi-Max *(Worldwide Interoprability for Microwave Access)*

El sistema Wi-Fi, el cual permite la creación de redes de trabajo sin el uso de cables, podría ser sustituido por el sistema Wi-Max, con grandes avances técnicos en cuanto a velocidad, alcance e interoperabilidad.

Las ventajas de la tecnología Wi-Max, comparadas con el actual sistema de redes Wi-Fi son muchas. Mientras el alcance de una señal Wi-Fi es de 200 metros en promedio, los sistemas Wi-Max podrían llegar a los 50 kilómetros. Además, su

rendimiento pensado para varios miles de usuarios conectados simultáneamente es considerablemente elevado.

Esta norma utiliza frecuencias de 2 a 11 Ghz con potencia suficiente para ofrecer altos rendimientos, la tecnología Wi-Max fue concebida desde un inicio, para convertirse en la red estándar a nivel internacional. Por ello, estas redes deberían ser compatibles en Estados Unidos y Europa. Esta compatibilidad permitirá que en el futuro, los usuarios que cuenten con este tipo de conexión puedan seguir utilizando su terminal. Por otro lado, los fabricantes de productos electrónicos tales como Intel, podrán crear chips para un mercado global.

Este criterio es determinante para los industriales, ya que permitirá que los precios bajen rápidamente. En un primer momento, las redes Wi-Max funcionarán como terminales conectadas a la internet, cada una de estas terminales tendrá capacidad para varios cientos de usuarios, que funcionarán como puntos de acceso de las redes de las empresas o de las terminales Wi-Fi. Para mayor detalle ver [10].

Bluetooth y Wi-Fi

La tecnología Bluetooth, ofrece una conectividad espontánea a los dispositivos móviles de los usuarios y permite el acceso instantáneo a la red utilizando puntos de acceso LAN y WAN. Trabajando con tecnologías complementarias, estos estándares asegurarían un acceso simple, inmediato y continuo a la información.

Bluetooth y Wi-Fi, son tecnologías totalmente complementarias. Las soluciones Bluetooth están diseñadas para redes personales con mayor énfasis en la movilidad y economía. Estas soluciones permiten conectar todos los aparatos Bluetooth, tales como : Computadoras portátiles, dispositivos de mano, teléfonos celulares y otros. Además se tendrá acceso parcial a la LAN y WAN, a través del punto de acceso. Para mayor detalle ver Cap. III [4].

1.10 Organismos Reguladores

Dentro de los organismos reguladores de mayor trascendencia respecto al desarrollo de los estándares y especificaciones técnicas para la implementación de redes inalámbricas podemos mencionar los siguientes

Institute of Electrical and Electronic Engineers (IEEE)
The Internet Engineering Task Force (IETF)
The Wi-Fi Alliance (WECA)

IEEE – Institute of Electrical and Electronic Engineers

El Instituto de Ingeniería Eléctrica y Electrónica (IEEE), es una asociación profesional técnica compuesta por más de 360 000 miembros en aproximadamente 175 países. El IEEE es la autoridad principal reguladora en áreas técnicas que van desde el diseño de computadoras, tecnología biomédica y telecomunicaciones.

A través de sus publicaciones técnicas, conferencias y actividades basadas en estándares activos produce el 30% de la literatura publicada en el mundo de la ingeniería y la tecnología. La IEEE cuenta con aproximadamente 900 estándares activos y 700 en desarrollo. Para mayor detalle ver [9].

IETF – The Internet Engineering Task Force

La IETF es una gran comunidad internacional de diseñadores de redes, operadores, vendedores e investigadores que tienen relación con la evolución de la arquitectura y funcionamiento de la internet. El trabajo técnico real del IETF es conformar grupos de trabajo organizados para analizar distintos temas como asignación de ruta, transporte, seguridad, etc.

La IETF es el grupo principal comprometido en el desarrollo de nuevas especificaciones estándares para la internet. Para mayor detalle ver [7].

WECA - The Wi-Fi Alliance

La Alianza Wi-Fi es una asociación internacional no lucrativa formada en 1999 para certificar la interoperabilidad de los productos de las WLAN basadas en especificación 802.11. Actualmente la alianza Wi-Fi tiene aproximadamente 200 compañias y más de 1500 productos que han recibido la certificación Wi-Fi .

La meta de los miembros de la alianza es reforzar la experiencia del usuario a través de la interoperabilidad de los productos. Para mayor detalle ver [8].

CAPÍTULO II
MARCO LEGAL

El objetivo de este capítulo es definir los aspectos y las normas legales a tener en cuenta en el diseño e implementación de nuestra red inalámbrica, ya que de omitirse alguna de estas consideraciones los organismos reguladores podrían suspender o cancelar la puesta en marcha de nuestro proyecto.

2.1 Aspectos Legales

Dada la problemática actual entorno a las Radiaciones No Ionizantes, no solo el Ministerio de Transportes y Comunicaciones se ha pronunciado sobre este tema, sino que también ahora otros organismos sin conocimiento de causa desean normarlo. Tal es el caso de los municipios distritales, defensa civil, digesa, entre otros, que tomando atribuciones que no les corresponden están transgrediendo sus propias facultades e invadiendo las de otros.

La intención de querer normar este tema es buena, porque anteriormente ningún ente las regulaba, el problema estriba en que primero debe definirse cuales serán los entes competentes y sus atribuciones respectivamente para poder empezar con la normalización.

Primero se dio un importante paso en el tema con la promulgación de la Ley General de Telecomunicaciones y luego con el Decreto Supremo N° 038-2003-MTC se han establecido los limites máximos permisibles de radiaciones no ionizantes en las telecomunicaciones, actualmente el ente encargado de realizar las mediciones es el INICTEL.

En este caso, por tratarse de un proyecto para uso interno únicamente, utilizándose equipos que trabajan en la frecuencia de 2.4 Ghz y que poseen antenas con potencias menores a los 10 dBm, esta exceptuado de ser incluido por esta norma.

Es importante recalcar que el tema legal en cualquier proyecto es bastante complejo y se debe tener especial cuidado, porque de omitirse cualquier norma, retrasaría la puesta en marcha del mismo. Para mayor detalle ver [12].

2.2 Propuesta técnica para el diseño de la red

La propuesta técnica presentada tiene las siguientes características:

- Es para uso interno de la Universidad Nacional de Ingeniería.
  Los equipos inalámbricos utilizados consumen potencias menores a 10 dBm (es decir, no dañan la salud).
- La frecuencia utilizada es de 2,4 Ghz, recientemente liberada por el MTC de la concesión que fuera brindada a la empresa Digital Way.

Por lo tanto, debemos tener en cuenta las siguientes consideraciones:

Reglamento General de la Ley de Telecomunicaciones, Decreto Supremo Nº 06-94-TCC, y modificatorias (Nºs. 005-98-MTC, 022-98-MTC, 002-99-MTC, 003-99-MTC, 043-2000-MTC, 029-2001-MTC, 029-2002-MTC y 015-2003-MTC; publicado el 19-03-2004).

Artículo 25º.- Están exceptuados de la clasificación de servicios de la ley, del reglamento y de los reglamentos específicos que se dicten, las telecomunicaciones instaladas dentro de un mismo inmueble que no utilizan el espectro radioeléctrico y no tienen conexión con redes exteriores.

También, están exceptuados de contar con concesión, salvo el caso del numeral 4, de la asignación del espectro radioeléctrico, autorización, permiso o licencia, para la prestación de servicios de telecomunicaciones, de la clasificación de servicios de la ley, del reglamento y de los reglamentos específicos que se dicten:

1. Aquellos servicios cuyos equipos, utilizando el espectro radioeléctrico, transmiten con una potencia no superior a 10 milivatios (mW) en antena (máxima potencia efectiva irradiada).

   Dichos servicios no podrán operar en las bandas de frecuencias atribuidas a los servicios públicos de telecomunicaciones; salvo en las bandas de frecuencias 2400-2483,5 MHz y 5725-5850 MHz.

2. Aquellos servicios cuyos equipos, utilizando una canalización establecida en la banda 462,550-462,725 MHz y 467,550-467,725 MHz, transmiten con una potencia no superior a 500 milivatios (mW) en antena (máxima potencia efectiva irradiada).

   Dichos equipos no podrán ser empleados para la prestación de servicios públicos de telecomunicaciones.

3. Aquellos servicios cuyos equipos, utilizando las bandas de 902-928 MHz, 2400-2483,5 MHz y 5725-5850 MHz, transmiten con una potencia no superior a 100 milivatios (mW) en antena (máxima potencia efectiva irradiada), y no son empleados para efectuar comunicaciones en espacios abiertos. Dichos servicios no deberán causar interferencias a concesionarios de servicios públicos de telecomunicaciones.

Sin perjuicio de lo dispuesto, aquellos que hagan uso de las frecuencias antes indicadas deberán respetar las normas técnicas emitidas o que emita el Ministerio.

DIRECTIVA QUE ESTABLECE LAS CONDICIONES DE OPERACIÓN DE LOS SERVICIOS QUE UTILIZAN LAS BANDAS DE 902-928 MHz, 2400-2483,5 MHz y 5725-5850 MHz.

Artículo 2°.- ALCANCES

La presente Directiva se aplica a la operación de los equipos que utilicen las bandas de frecuencias de 902 - 928 MHz, 2400 - 2483,5 MHz y 5725 - 5850 MHz, los cuales deberán sujetarse a las características técnicas establecidas en el Artículo 4°.

Artículo 4°.- CARACTERÍSTICAS TÉCNICAS DE OPERACIÓN

Los servicios que operen bajo los alcances de la presente Directiva deberán cumplir con las siguientes características:

1. La potencia pico máxima de salida de un transmisor no debe exceder 1,0 vatio, sea que se trate de un servicio fijo o móvil. El transmisor deberá estar instalado en un ambiente de fácil acceso a fin de facilitar la labor de supervisión por parte del Ministerio.

2. Para el servicio privado:
   En las ciudades solo estarán permitidos enlaces punto a punto utilizando antenas directivas, con un ancho de lóbulo no mayor de 30°, salvo para el caso de las aplicaciones de recinto cerrado en redes de área local.
   En las áreas rurales, lugares considerados de preferente interés social y lugares geográficamente aislados de las zonas urbanas en las ciudades, las antenas podrán ser sectoriales y omnidireccionales.

3. Para el caso de los servicios públicos en enlaces punto a punto las antenas deberán ser directivas, con un ancho de lóbulo no mayor de 30° y en el caso de enlaces punto multipunto las estaciones base podrán emplear antenas sectoriales con un ancho de lóbulo de hasta 90°. En las áreas rurales y en lugares considerados de preferente interés social las antenas podrán ser omnidireccionales.

4. La potencia isotrópica radiada equivalente máxima (PIRE), deberá sujetarse a las características que se muestran en la Tabla 2.1

Notas:

En el caso de los equipos que operen en las bandas de 2400 - 2483,5 MHz y 5725 - 5850 MHz en zonas rurales, están permitidos mayores valores de la PIRE, empleando antenas directivas de mayor ganancia.

En ningún caso se deberán emplear transmisores que excedan la potencia a 1,0 vatio.

Tabla 2.1 Potencias Isotrópicas Radiadas Equivalentes (PIRE)

Banda de Operación	**PIRE máxima**
902-928 MHz	30 dBm / 1 W
2400-2483,5 MHz	36 dBm / 4 W
5725-5850 MHz	36 dBm / 4 W

Artículo 5°.- MODALIDADES DEL SERVICIO

Las aplicaciones de los servicios de telecomunicaciones que operen bajo los alcances de la presente directiva deberán sujetarse a las siguientes modalidades:

Banda 2400 – 2483,5 MHz

1. Punto a punto.
2. Punto a multipunto, solamente en áreas rurales, en lugares considerados de preferente interés social o lugares geográficamente aislados de las zonas urbanas de las ciudades.

3. Recinto cerrado para utilización exclusiva dentro de edificaciones sin cruzar vías públicas, en redes de área local.

Otras bandas de frecuencia usadas en telecomunicaciones

13553 - 13567 KHz (frecuencia central 13560 KHz),
26957 - 27283 KHz (frecuencia central 27120 KHz),
40,66 - 40,70 MHz (frecuencia central 40,68 MHz),
902 - 928 MHz (frecuencia central 915 MHz),
2400 - 2500 MHz (frecuencia central 2450 MHz),
5725 - 5875 MHz (frecuencia central 5800 MHz), y
24 - 24,25 GHz (frecuencia central 24,125 GHz)

Estas bandas están destinadas para aplicaciones industriales, científicas y médicas (ICM). Los servicios de radiocomunicaciones que funcionan en estas bandas deben aceptar la interferencia perjudicial resultante de estas aplicaciones y en ningún caso podrán causar interferencias a las aplicaciones ICM.

Por lo tanto, no se necesita tramitar ningún permiso en el Ministerio de Transportes y Comunicaciones ni en la municipalidad del distrito.

CAPÍTULO III
APLICACIÓN

El objetivo de este capítulo es detallar brevemente los parámetros necesarios para el diseño e implementación de nuestra red inalámbrica, analizando la eficiencia, adaptación al medio, seguridad y los costos de instalación, dependiendo del tipo de conexión y/o aplicación.

La intención final es crear a futuro una gran red, mediante la unión de pequeñas redes, libres e independientes.

3.1 Implementación de la red Wi-Fi en la Facultad de Ingeniería Eléctrica y Electrónica de la Universidad Nacional de Ingeniería.

La primera fase del proyecto esta constituida por un estudio pormenorizado de las distintas tecnologías y estándares inalámbricos.

Para la arquitectura de nuestra red Wi-Fi, se ha optado por la implementación de una red inalámbrica bajo el estándar 802.11g a 54 Mbps en modo infraestructura, el identificador de la red Wi-Fi o SSID de los puntos de acceso sería WIFI_FIEE.

La red se ha diseñado con 5 puntos de acceso ubicados dentro de la Facultad de Ingeniería Eléctrica y Electrónica (FIEE), 4 puntos de acceso destinados para el uso de los alumnos, profesores, investigadores y personal de servicio, y un quinto punto ubicado en el nodo Wi-Fi, para aplicaciones de prueba y desarrollo.

La distribución sería de la siguiente manera :

1 punto de acceso ubicado en la biblioteca de cada uno de los pisos de la facultad (3 pisos).
1 punto de acceso en el salón de docentes, investigadores y personal de servicio.
1 punto de acceso en el nodo Wi-Fi (para desarrollo y pruebas).

Se ha elegido una red 802.11g con puntos de acceso modelo 3Com7250, se ha optado por este dispositivo por sus características técnicas y su buena relación calidad precio.

Para el nodo Wi-Fi, se ha considerado la instalación de un servidor IBM x Series225, con sistema operativo Linux cuyas funciones básicas son

Servidor de autentificación.
Servidor HTTP y FTP.
Configuración de direccionamiento IP.
Router y Firewall.

El nodo de acceso a la red Wi-Fi, será montado en forma de Gateway con 2 interfaces de red, una conectada a la red wireless y la otra conectada a la red Ethernet de la Universidad Nacional de Ingeniería (UNI), separandolos por completo, mediante una LAN virtual (VLAN) la red Wi-Fi de la red de la universidad, permitiendo el acceso sólo a las personas o usuarios autorizados, previa autentificación determinada en nuestra red; para tal efecto se implementarán los siguientes mecanismos de seguridad :

Autentificación de usuarios mediante un portal cautivo integrado con el servicio de autentificación de la universidad.
Software de detección de intrusos.
Servicio de monitorización de la red.

La interconexión de los puntos de acceso se realizará mediante una VLAN (Red de Area Local Virtual) dentro de los switches de conmutación de la universidad, tal como se muestra en la Fig. 3.1.

Una VLAN puede definirse como un conjunto de dispositivos conectados en red, que a pesar de estar físicamente conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distintas, diferentes pisos, e incluso distintos edificios, pertenecen a una misma LAN.

Las características principales de la VLAN son :

Direccionamiento de una IP privada.
Servidor DHCP integrado en la red VLAN (Nodo Wi-Fi).
Las direcciones de la VLAN no serán accesibles desde el exterior (Internet).
Necesidad de autentificación para acceder a la red pública de la UNI.
Alimentación de los puntos de acceso mediante PoE *(Power Over Ethernet)*.

La interfaz pública del Gateway tiene asignada una dirección IP estática, la cual estará asociada a un subdominio y dará de alta a los servidores de nombres de la universidad.

Las características del Gateway son

Direccionamiento IP interfaz pública.
Subdominio asociado. Ejemplo : wififiee.uni.edu.pe.

Los puntos de acceso estarán ubicados dentro de la facultad de tal forma que el área que cubra cada punto, se solapen lo menos posible con los puntos adyacentes, a la vez que se maximice su alcance.

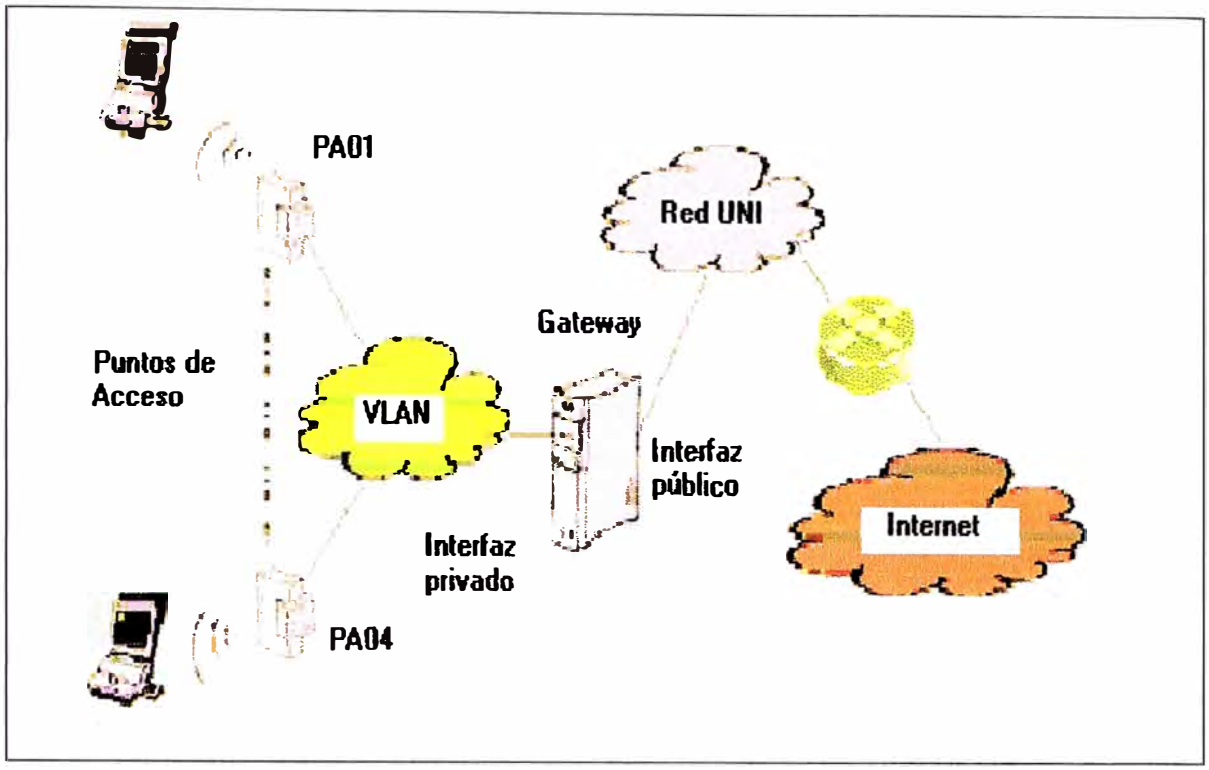

Fig. 3.1 Interconexión entre la red Wi-Fi y la red de la UNI

3.1.1 Conexión a la VLAN

Los puntos de acceso y la interfaz privada del Gateway se conectarán mediante una VLAN, soportada por los switches de la universidad. Esta VLAN permite aislar el tráfico de la red Wi-Fi del resto de tráfico de red de la universidad, disponiendo de un direccionamiento IP reservado para los clientes inalámbricos.

Los switches están instalados en los repartidores (racks) que el servicio de infraestructuras dispone en la facultad. Los racks mediante cableado estructurado Ethernet, permiten flexibilizar las conexiones entre los puntos de red (RJ45) y los puertos del switch.

Para la instalación del Gateway se ha optado por un servidor IBM x Series225 con sistema operativo Linux y un software que permita autenticar el acceso a la red vía un portal cautivo, en nuestro caso usaremos el software NoCatAuth, el NoCat es un software escrito en lenguaje Perl. Este portal cautivo se usará para controlar el acceso de los usuarios a la red Wi-Fi, el cual estará compuesto por un Gateway y un servidor de autenticación.

Cuando un usuario de la red Wi-Fi se ha asociado y desea navegar, tiene que cursar su tráfico a través del Gateway, en ese momento NoCatAuth solicita la acreditación al usuario, y si esta es positiva le permite al usuario navegar con las restricciones asociadas a su perfil (alumno, docente, investigador, etc.).

La autentificación se realizará mediante el identificador del usuario, el cual se validará en forma online con los servidores de la universidad, lo cual permitirá un sistema de control personalizado y actualizado en todo momento.

Inicialmente se podría establecer la navegación en la red Wi-Fi de la siguiente forma :

Profesores e investigadores de la UNI con perfil "Docente".
Personal auxiliar y de servicio de la UNI con perfil "PAS".
Alumnos de la facultad con perfil "Alumno".
Equipo de investigación del proyecto con perfil "Desarrollo".

Los posibles resultados que pueden obtenerse con respecto a la velocidad para suministrar datos operando bajo el estándar 802.11g se muestran a continuación :

Tabla 3.1 Anchos de Banda bajo el estándar 802.11g

Tipo / 802.11g	Ancho de banda Teórico	Posible Ancho de banda Resultante
Texto	54 Mbps	22,24 Mbps
WEP 64	54 Mbps	20,96 Mbps
WEP 128	54 Mbps	20,96 Mbps

Como puede observarse en la tabla superior, en la práctica no se consigue la velocidad teórica de la red. En concreto, el protocolo 802.11g tiene un ancho de banda medio de aproximadamente 22 Mbps frente a los 54 Mbps teóricos.

Este diseño podría generalizarse para la conexión de otras redes Wi-Fi implementadas en otras facultades de la Universidad Nacional de Ingeniería.

3.1.2 Detalles y especificaciones técnicas de los componentes Wi-Fi

Puntos de Acceso 3Com 7250

Como se ha indicado anteriormente, para el diseño e implementación de este proyecto se han utilizado puntos de acceso modelo 3Com7250, cuyas características y especificaciones son las siguientes :

- Velocidad de transmisión de datos : Hasta 54 Mbps.
- Soporta encriptación WPA, AES y WEP.
- Autentificación por MAC.
- Claves dinámicas de acceso por sesión.
- Autenticación Radius 802.1x.
- Claves de encriptación pública TKIP y EAP.
- Ofrece roaming entre puntos de acceso.

Selección automática de canales.
Soporta hasta 253 usuarios simultáneamente.
Tiene un alcance de hasta 100 metros en transmisión y recepción.
Protocolo de acceso a medios : CSMA/CA
Opciones de antena externa disponible.
Es compatible con el estándar 802.11b.
Dimensiones : 20.5 cm de alto, 22 cm de ancho y 8 cm de fondo.

Estos puntos de acceso disponen de un puerto Ethernet 10/100 y de un puerto serie para su administración local, así mismo disponen de una entrada de alimentación de corriente continua de 3.3 v. También pueden recibir alimentación eléctrica mediante el cable de red Ethernet (estándar PoE) que los conecta a las VLAN, evitando de esta forma llevar electricidad (220V CA) hasta los puntos de acceso, los cuales deben estar ubicados en lugares poco accesibles.

El estándar Power over Ethernet (PoE) permite que un inyector de alimentación, inserte tensión en corriente continua (48V CC) en los pares no utilizados del cable trenzado. Existen dos tipos de inyectores, en forma individual (usado en nuestro proyecto) o en formato múltiple o hub, este último permite alimentar varios puntos de acceso.

Servidor IBM x Series 225

Este servidor de dos vías aporta un valor excepcional a los grupos de trabajo al combinar características de rendimiento estable con nuevas funciones de disponibilidad a bajo precio. A continuación detallaremos algunas especificaciones técnicas

Formato : Torre o bastidor de 4U
Procesador : Intel Xeon de 3,06 Ghz
Memoria : Chip Drill DDR de 256MB o 512/8 GB

Ranuras de expansión : 5 en total / 4 PCI-X

Red : Ethernet 10 / 100 / 1000 integrada

Sistemas operativos soportados : Windows Server 2003, Windows 2000 Advanced Server, Red Hat Linux, Linux Professional 8,0 y Novell Netware.

Adaptadores de Red Inalámbricas

Actualmente en el mercado existe una gran variedad de tarjetas inalámbricas para acceder a una red Wi-Fi, en nuestro caso hemos considerado el uso de tarjetas marca D-link (D-Link DWL-G650) tipo PCI, por su bajo costo, alto rendimiento y compatibilidad con los equipos usados en el diseño de la red.

A continuación detallaremos sus principales características

Velocidad de transmisión de hasta 54 Mbps en 2,4 Ghz

Compatible bajo el estándar 802.11b y 802.11g

Seguridad avanzada WPA y 802.1x

Formato de código de línea : CCK, BPSK, QPSK

Cobertura máxima : 100 metros en interiores, 400 metros al aire libre.

Antena externa desmontable.

Dimensiones : 14.1cm de alto, 1.9cm de ancho y 15.2 cm de profundidad.

Antenas de Red Inalámbrica (Opcional)

En algunas redes inalámbricas, es necesario la instalación de antenas para conseguir una señal uniforme en puntos alejados. Para acceder a nuestra red se podría utilizar una antena omnidireccional ANT24-0700, dotada de una ganancia de 7 dBi para obtener una mejor recepción.

Características y especificaciones técnicas :

- Funciona con cualquier periférico que responda a la norma 802.11g con un conector SMA o TNC
- Para facilidad de uso, incluye una base magnética con un cable de extensión de 1.5 metros.
- Nos permite ahorro de costes de un repetidor o punto de acceso suplementario.
- Gama de frecuencia : 2,4 a 2,5 Ghz.
- Ganancia : 7 dBi
- Radio de alcance : 24°

3.1.3 Precios referenciales de los componentes Wi-Fi

- Puntos de Acceso modelo 3Com7250 : De $150.00 a $250.00 dependiendo de las ventajas del equipo.

- Servidor IBM x Series 225 : De $ 1000.00 a $ 1500.00 dependiendo de la cantidad de memoria y capacidad de almacenamiento.

- Adaptadores o tarjetas inalámbricas : Desde $ 30.00 hasta $ 100.00 dependiendo de la marca y el modelo. En nuestro caso los precios de las tarjetas D-Link son los siguientes :
  Adaptadores PCMCIA D-Link : De $ 30.00 a $ 40.00
  Adaptadores USB D-Link : De $ 20.00 a $ 30.00

- Antenas Omnidireccionales : De $ 50.00 a $ 150.00. El precio de las antenas para redes Wi-Fi, varían según la ganancia y la cobertura.
  Para nuestro diseño podemos usar la antena D-Link modelo ANT24-0700 cuya ganancia es de 7 dBi . Su valor en el mercado es de $ 70.00

3.1.4 Modelo y Costos de la Aplicación

4 Puntos de Acceso modelo 3Com serie 7250
Estándares : 802.11g y 802.11b
Costo : 4 x $ 200.00 = $ 800.00

1 Servidor IBM Serie 225
Procesador Intel Xeon 3,06 Ghz
Memoria Chip Drill DDR de 512 MB
Costo : $ 1200.00

Antena Omnidireccional Modelo ANT24 – 0700
Ganancia : 7 dBi , estándar 802.11g. Radio de alcance : 24 grados.
Costo : $ 70.00

Cables, conectores y gastos complementarios $ 30.00

COSTO TOTAL APROXIMADO : $ 2100.00

CONCLUSIONES

1. Para el diseño e implementación de la red Wi-Fi, se recomienda la utilización del estándar 802.11g, por ser uno de los estándares más difundidos en la actualidad, además de la compatibilidad existente con el estándar 802.11b.

2. En cuanto al tema de la seguridad, la elección del método de autenticación es una decisión fundamental, así como también la elección del servidor de autenticación y del software de los clientes.

3. En cuanto al tema económico, la inversión no es grande, teniendo en cuenta que se han realizado trabajos de cableado estructurado dentro de la universidad., siendo únicamente necesaria la adquisición, instalación y configuración de los equipos y programas anteriormente mencionados.

4. Inicialmente se tomarán como áreas piloto la Facultad de Ingeniería Eléctrica y Electrónica (FIEE), posteriormente el proyecto podrá ser aplicado a las demás facultades de la universidad así como también a los edificios administrativos.

5. En cuanto al tema legal, puesto que se trata de un proyecto para uso interno y exclusivo de la Universidad Nacional de Ingeniería, los equipos inalámbricos utilizados consumen potencias menores a 50 mW (no dañan la salud), y la frecuencia utilizada es la de 2,4 Ghz, recientemente liberada por el MTC de la concesión que le fuera brindada a la empresa Digital Way, no será necesario realizar tramite alguno con el MTC ni con el municipio del distrito.

6. Considerando que en el futuro la tecnología pueda adquirir grandes avances tecnológicos en velocidad, alcance e interoperabilidad, debemos aclarar que ambas tecnologías son complementarias y su sinergia permitirá la utopía de la conectividad desde cualquier lugar y desde cualquier dispositivo. Wi-Max no sustituirá a las redes Wi-Fi, sino que coexistirán, hasta que en algún momento la tecnología Wi-Max se imponga sobre la tecnología Wi-Fi .

7. Wi-Fi ofrece una cobertura de 200 a 900 metros con algunas tecnologías. WI MAX por su parte permite una cobertura de hasta 50 Km y puede atender hasta 1552 usuarios residenciales por antena, con velocidades de hasta 55 Mbps. Hoy Wi-Max no es un estándar y tiene limitaciones en la movilidad, porque el Wi-Max actual sólo soporta velocidades de 55 km por hora, para ofrecer voz sobre IP

8. Bluetooth y Wi-Fi pueden trabajar juntos para permitir que los usuarios tengan acceso a su información, a cualquier hora y desde cualquier lugar. El Bluetooth será utilizado como el reemplazo de los cables y como un medio de comunicación en aparatos con restricciones de potencia y tamaño, tales como teléfonos celulares, dispositivos de mano, cámaras, bocinas, auriculares y otros más. Wi-Fi será usada para extender o reemplazar a las LAN's por cable, brindando acceso a la Internet y una gama completa de características LAN a los usuarios, sin la necesidad del uso de cables. Además, son fác de instalar y hacen que las redes en el hogar sean más razonables.

GLOSARIO

A

Ad Hoc

Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".

AES - Estándar de Cifrado Avanzado AES - Advanced Encryption Standard

También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando al hasta entonces estándar DES.

Amplificador Amplifier

Produce un incremento significativo en el alcance de la señal de las WLAN. Consta de un receptor de bajo ruido pre-amplificado y un amplificador lineal de salida de radio frecuencia (RF).

Ancho de Banda Bandwidth

Este término define la cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado.

Antena Antenna

Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia que punto emitan la señal podemos encontrarlas direccionales u omnidireccionable.

Appliance Server

Servidores (dedicados a Internet sharing, servicios FTP, e-mail, conexiones VPN, servicios de cortafuegos, de impresora y archivo y también operan como servidores web) que incorporan hardware y software en el mismo producto de modo que todas las aplicaciones se encuentran preinstaladas.

B

Bluetooth

Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, ratones, etc....) que implementen esta tecnología ya que su FHSS/Hopping Pattern es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras.

Bridge (Puente)

Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.

C

Centrino

Tecnología móvil desarrollada por Intel compuesta por un procesador Pentium M, chipset 855 y conectividad inalámbrica integrada.

CHAP - Challenge Handshake Authentication Protocol

CHAP

Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, mucho más seguro que el PAP.

Cliente Inalámbrico

Wireless Client

Toda solución susceptible de integrarse en una red wireless como PDA's, portátiles, cámaras inalámbricas, impresoras, etc.

D

Dirección MAC - Control de Acceso a Medios

MAC - Media Access Control Address

Dirección hardware que identifica únicamente cada nodo de una red. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red.

Dispositivo Móvil (DM)

Ya sea Tarjeta PCMCIA, USB, PCI (Slot de un PC de sobremesa), Centrino, que sustituyen a las tarjetas de red. Su función es la de recibir y enviar información desde la estación en que están instaladas (portátiles, PDA's, móviles, cámaras, impresoras, etc).

DSSS - Espectro Amplio mediante Secuencia Directa

DSSS - Direct Sequence Spread Spectrum

A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores: cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos.

E

EAP - Protocolo de Autenticación Extensible

EAP - Extensible Authentication Protocol

Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros.

Estándar

Standard

Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc.

Estándar 802.11a

802.11a standard

Opera bajo la frecuencia de los 5 GHz y permite alcanzar velocidades de 54 Mbps. Sin embargo, en algunos países no tiene vigencia al estar su frecuencia restringida a entornos militares y otros ámbitos.

Estándar 802.11b

802.11b standard

Trabaja en la frecuencia de los 2.4 GHz, con 13 canales disponibles y posibilita velocidades de 11 Mbps en su primera versión y 22 Mbps en su edición Plus.

Estándar 802.11g

802.11g standard

Protocolo de comunicación inalámbrica aprobado en abril de 2003 que faculta a operar a 54 Mbps en la frecuencia de los 2.4 Ghz.

F

FHSS - Espectro Amplio mediante Saltos de Frecuencia

FHSS - Frequency Hopping Spread Spectrum

Primer desarrollo de la técnica de transmisión del Espectro Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí.

G

Gateway (Pasarela/Puerta)

Dispositivo que funciona como puerta de enlace entre la Internet y las redes inalámbricas.

GPS - Sistema de Posicionamiento Global

GPS - Global Position System

Sistema de navegación por satélite con cobertura global y continua que ofrece de forma rápida y temporalmente bastante precisa una posición geográfica de un elemento.

H

Hash

Un valor hash, también conocido como "message digest", es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados.

Hot Spot (Punto Caliente)

Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc), que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.

I

IEEE

Siglas del "Institute of Electrical and Electronic Engineers" (http://www.ieee.org) formado a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo.

IETF

Siglas de "The Internet Engineering Task Force" (http://www.ietf.org), grupo principal auto-organizado comprometido en el desarrollo de nuevas especificaciones estándares para Internet.

Infraestructura — Infrastructure

Topología de una red inalámbrica que consta de dos elementos básicos: estaciones cliente wireless y puntos de acceso.

IPsec - IP Security

Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPN's), soporta dos modos de encriptación: Transporte y Túnel.

L

LDAP - Protocolo de Acceso Ligero a Directorio — LDAP - Lightweight Directory Access Protocol

Protocolo para el acceso a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a la Internet.

LEAP

Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección.

M

Mbps (Megabits por segundo)

Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.

MD5

Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos.

MHz (Megahertzio)

Unidad empleada para medir la "velocidad bruta" de los microprocesadores equivalente a un millón de hertzios.

MS-CHAP - Protocolo de Autenticación por Desafío Mutuo

MS-CHAP - Challenge Handshake Authentication Protocol

Protocolo de autenticación utilizado por el acceso remoto de Microsoft y conexiones de red y de acceso telefónico. Con CHAP los clientes de acceso remoto pueden enviar de forma segura sus credenciales de autenticación a un servidor de acceso remoto.

O

802.11

Se refiere a una familia de especificaciones desarrollada por el IEEE y aprobada por ésta en 1997 para tecnologías de red inalámbricas y especifica un interfaz aéreo entre un cliente inalámbrico y una estación base o entre dos clientes wireless.

OFDM - Orthogonal Frequency Division Multiplexing

Técnica de modulación FDM (empleada por el 802.11a wi-fi) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

P

PAP - Protocolo de Autenticación de Claves

PAP - Password Authentication Protocol

El método más básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave. Típicamente, las contraseñas almacenadas en la tabla se encuentran encriptadas. El principal defecto de PAP es que tanto el nombre de usuario como la clave se transmiten sin codificar, a diferencia de sistema CHAP.

PEAP - Protected Extensible Authentication Protocol

Protocolo del tipo EAP desarrollado conjuntamente por Microsoft RSA Security y

Cisto para la transmisión datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red wi-fi empleando sólo certificados del lado servidor creando una túnel SSL/TLS encriptado entre el cliente y el servidor de autenticación. El túnel luego protege el resto de intercambios de autenticación de usuario.

PKI - Infraestructura de Clave Pública PKI - Public Key Infrastructure

Sistema de certificados digitales. Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet. Los estándares de PKI siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico. La infraestructura de claves públicas se llama también PKI.

Punto de Acceso (PA) Access Point (AP)

Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

R

RADIUS RADIUS - Remote Authentication Dial-In User Service

Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISP's) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

RAS - Servidor de Acceso Remoto RAS - Remote Access Server

Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

Roaming

(Itinerancia). En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad

S

Sniffers

Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información.

SSID

Identificador de la red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

SSL - Secure Sockets Layer

Aprobado como estándar por el The Internet Engineering Task Force (IETF), es un protocolo desarrollado por Netscape para la transmisión privada de documentos vía Internet cliente/servidor. Trabaja empleando una llave privada de encriptación de datos que es transferida a través de la conexión SSL.

T

Tarjeta de Red Inalámbrica

Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB

TKIP - Protocolo de Integridad de Clave Temporal

TKIP - Temporal Key Integrity Protocol

Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS - Transport Layer Security

Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet.

W

Warchalking

Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico. Tiene sus antecedentes durante la Gran Depresión del 30 en los Estados Unidos, los desocupados dibujaban símbolos en los edificios para marcar los lugares donde podían conseguir comida.

Wardriving

Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos wireless. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc.

WAP

Siglas de "Wireless Application Protocol", protocolo de aplicación de tecnología inalámbrica que posibilita el acceso a páginas web especialmente diseñadas para este lenguaje y está disponible en versiones 1.1 y 2.0.

WEP

Siglas del protocolo "Wired Equivalent Privacy", proporciona transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad.

Wi-Fi Alliance

"The Wi-Fi Alliance" se formó en 1999. Certifica la interoperabilidad de productos

WLAN basados en la especificación 802.11.

WIMAX

Siglas de "Worldwide Interoperability for Microwave Access" (http://www.wimaxforum.org), grupo no lucrativo formado en abril de 2003 iniciativa de Intel/Nokia/Fujitsu/entre otras que certifica la interoperabilidad de los productos con tecnología inalámbrica.

WLAN

Siglas de "Wireless Local Area Network" (Ver Red Inalámbrica).

WPA - Acceso Wi-Fi Protegido WPA - Wi-Fi Protected Access

Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WWWD

Siglas de "The WorldWide Wardrive", evento internacional que durante una semana reúne a expertos de todo el mundo que buscan y catalogan nodos inalámbricos en sus ámbitos geográficos (http://www.worldwidewardrive.org/).

BIBLIOGRAFÍA

[1] Andrew S. Tanenbaum, "Redes de Computadoras", Universidad Libre de Amsterdam, PrenticeHall, 1997.

[2] Bates,R.J, "Comunicaciones en Redes Inalámbricas", Universidad de New YorK, McGraw Hill, 1994.

[3] David Roldán Martinez, "Comunicaciones Inalámbricas, un enfoque aplicado", Universidad Politécnica de Valencia, 2004.

[4] Adam Engst; Glen Fleishman, "Introducción a las Redes Inalámbricas", Ed. Anaya Multimedia, 2003.

[5] Reid, Neil & Seide, Ron, "Manual de Redes Inalámbricas", Universidad de New YorK, McGraw Hill (1ra Edición), 2004.

[6] José Carballar Falcón, "Wi-Fi, Como Construir una Red Inalámbrica", Ed. Ra-ma, (2da Edición), 2004.

[7] http://www.ietf.org

[8] http://www.weca.net

[9] http://www.ieee.org

[10] http://www.wimaxforum.org

[11] http://www.wirelessethernet.com

[12] http://www.mtc.gob.pe/portal/comunicacion/concesion/mlegal