MODELO OSI CAPA 1 Y 2 WIRELESS

1 OBJETIVO

Hasta el momento hemos estado abordando el estudio de la comunicación en red realizando un paulatino ascenso en la estratificación propuesta por OSI. En la clase de hoy integraremos los conocimientos adquiridos hasta el momento y los aplicaremos al análisis de otro medio de comunicación como es Wireless.

Para lograr este objetivo, será necesario que tomemos conocimiento de todas las tecnologías involucradas y las normativas vigentes que rigen las redes Wireless, para poder seleccionar los productos adecuados, asegurar la compatibilidad técnica y operativa entre los diferentes tipos de productos.

2 INTRODUCCIÓN

Abordaremos el estudio de las redes Wireless como un complemento de las redes cableadas, y no como una competencia para estas.

Wireless puede ser utilizado para realizar extensiones topológicas en forma rápida y limpia. También son utilizadas habitualmente para la implementación en aquellos escenarios en los que las redes cableadas son inviables por distintas razones.

Las redes inalámbricas han crecido enormemente en los últimos años, con el objetivo de conectar de manera eficiente y rápida una PC a una red, ya sea publica (INTERNET) o privada (LAN). Los cables en algunos casos son un problema, con Bluetooth la flexibilidad de interconectar dos dispositivos sin depender de un cable es muy importante.

Como ejemplo, supongamos que hemos adquirido una nueva Cámara Digital de 3 Megapixels con la funcionalidad de Bluetooth y ya teníamos en nuestro haber una PC Portátil con soporte para esta tecnología, simplemente configurando unos parámetros podría transferir las fotos en un abrir y cerrar de ojos sin la necesidad de conectar ningún cable.

Hoy día existen dos grandes grupos en las comunicaciones inalámbricas, las cuales trataremos en este capitulo de actualización técnica, estos son: Bluetooth y WI-FI.

3 BLUETOOTH

Bluetooth es una tecnología que revoluciona la manera de interconectar dispositivos, y de poder acceder a la información de manera dinámica y fácil. Bluetooth es evidentemente una evolución de las transmisiones infrarrojas, cuyo funcionamiento no podía exceder un espacio físico determinado. El desarrollo de Bluetooth esta orientado a las necesidades de conectar dispositivos de manera sencilla, como Handhelds (Palm's, y Agendas), Telefonía Celular, Handsets (Auriculares inalámbricos y otros accesorios), PC, Notebooks, Teclados y Mouse, Impresoras y una gran cantidad de dispositivos.

Quienes llevan adelante el desarrollo de Bluetooth es un grupo de interés especial (SIG) formado por varias compañías de los sectores de las telecomunicaciones, informática y fabricantes de chips, entre las que se encuentran: Ericsson, IBM, Intel, Nokia y Toshiba.

Características técnicas:

- Ancho de Banda (Bandwidth): 1MB/s, 432 KB/s funcionando a full duplex, 721/56 Kb/s para transmisiones asimétricas.
- Las coberturas de trabajo van desde los 10 a los 100 metros según las disponibilidades de cada dispositivo.
- Trabaja en un rango de frecuencia de 2,4 a 2,8 GHz.
- Soporta transmisiones de datos y voz.
- Los dispositivos no necesitan estar “visibles” en algunos casos, para poder comunicarse.
- Soporta niveles de encriptación de datos para obtener mayor seguridad en la transmisión de datos.

3.1 ¿COMO TRABAJA?

El rango de frecuencia de Bluetooth como dijimos más arriba opera en una banda no licenciada desde los 2,4 GHz. hasta los 2,8 GHz., esta banda es de libre utilización para ISM (Instrumental, Medical & Scientific) y también es el rango de frecuencia en el que operan los hornos microondas, entonces las Handhelds se verán afectadas algunas veces en presencia de un dispositivo de estas características que no cumpla con las normas de seguridad preestablecidas para estos.

Como el rango de operación involucra más de una frecuencia de trabajo, son los dispositivos los que deben elegir la frecuencia exacta en la que van a comunicarse, utilizando lo que se llama Spread Spectrum y Frequency Hopping. Pasemos a explicar estos dos términos: Spread Spectrum (espectro extendido) es la capacidad de poder trabajar en un espectro extendido de frecuencia. Frequency Hopping (saltos de frecuencia) es justamente, como su nombre lo indica, la habilidad de saltar de frecuencia en intervalos regulares, en este caso lo hace hasta 1600 saltos por segundo.

Entonces estas dos características hacen que Bluetooth tenga un alto grado de inmunidad a las interferencias, puesto que si está operando en una frecuencia determinada y esta se ve interferida por otra señal, rápidamente los dispositivos se ponen de acuerdo en trabajar en otra.

Este es el primer paso para que dos dispositivos Bluetooth se comuniquen, pero faltan algunos puntos para poder transmitir datos entre sí.

El próximo paso es el de tener habilitado un *Perfil* (Profile en Inglés), y que este perfil sea compatible con el del otro dispositivo. Pasemos entonces a profundizar este método de trabajo. Un perfil es una serie de implementaciones, que incluyen que tipo de protocolos debe usar cada dispositivo, para dar una serie de funciones que necesita este *perfil*, a su vez el otro o los otros dispositivos que se comunicarán con este tendrán cada uno su perfil definido, pero deben soportar (o entender) el *Perfil* del primero para poder establecer la comunicación. Entonces podríamos definir un *perfil* como el "comportamiento" que debe tener cada dispositivo. Ahora pasaremos a describir los perfiles más comunes que están en vigencia en estos tiempos, ya que los desarrolladores de esta tecnología incorporan a las especificaciones de la norma nuevos perfiles según las necesidades actuales (la norma en vigencia es la 2.0).

Existen cuatro Perfiles en los cuales están sustentados los demás, llamados perfiles fundamentales:

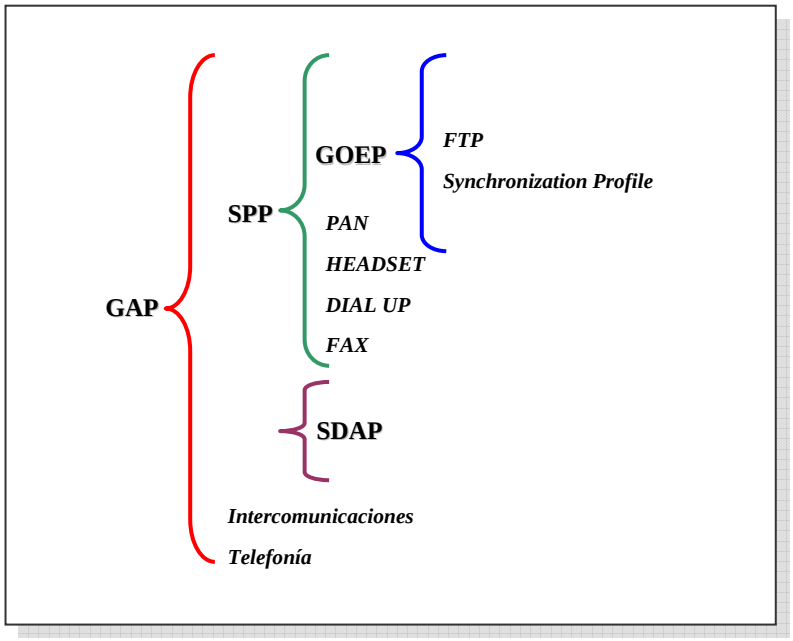
3.1.1 Perfiles Fundamentales:

- GAP (**G**eneral **A**ccess **P**rofile) Perfil de Acceso General, describe como dos dispositivos deben comunicarse para cumplir funciones básicas. Este protocolo debe ser soportado por las aplicaciones que necesitan intercambiar datos.
- SPP (**S**erial **P**ort **P**rofile**)** Describe como el dispositivo debe simular un puerto serial para que algunas aplicaciones funcionen a través de esta comunicación. Este a su vez depende del perfil GAP.
- SDAP (**S**ervice **D**iscovery **A**pplication **P**rofile) Perfil de descubrimiento de servicio de aplicación Enumera la cantidad y los tipos de servicio que pueden ser provistos a través de los enlaces Bluetooth y que aplicaciones serán usadas para esta comunicación. El perfil SDAP es dependiente del Perfil GAP.
- GOEP (**G**eneral **O**bject **E**xchange **P**rofile) Perfil general para el intercambio de objetos. Este perfil define en líneas generales los protocolos y procedimientos que serán utilizados para el intercambio de objetos. Ej.: transferencia de archivos. El perfil GOEP depende del perfil Serial Wireless Profile.

3.1.2 Perfiles de trabajo o también llamados modos de uso:

- Cordless Telephony Profile (Perfil de telefonía inalámbrica) describe por ejemplo, como un teléfono celular debe comunicarse con un Headset, que es un dispositivo que permite utilizar el teléfono con manos libres.
- Intercom Profile (Perfil de Intercomunicación). Este perfil define como dos o más teléfonos celulares pueden establecer comunicación entre sí sin utilizar la red de telefonía.
- Headset Profile Define como deben comportarse estos dispositivos con otro similar o por ejemplo con un teléfono celular.
- Dial-Up Networking Profile (Perfil de comunicación telefónica entre computadoras) Es principalmente como se realiza una conexión vía MODEM telefónico que puede ser establecida desde un equipo como una notebook hacia un teléfono celular.
- Fax Profile (Perfil de FAX) está basada en la anterior pero con el agregado de poder enviar y recibir FAX.
- LAP - **L**AN **A**ccess **P**rofile (Perfil de Acceso a redes LAN) Define como debe interconectarse hacia una red LAN (cableada) pudiendo utilizar la comunicación a Internet de la misma, utilizando el protocolo PPP (Point to Point Protocol - Protocolo Punto a Punto).
- FTP –**F**ile **T**ransfer **P**rofile (Perfil de Transferencia de Archivos) define como transferir archivos entre dos dispositivos Bluetooth.
- Advanced Audio Distribution Profile (Perfil de Distribución avanzada de Audio) define como los dispositivos deben intercambiar información referida al audio entre sí, como por ejemplo entre un micrófono (o cualquier otra fuente de entrada en el proceso de grabación), un reproductor portátil o un par de auriculares (proceso de reproducción).
- Basic Printing Profile (Perfil Básico de Impresión). Define como los dispositivos imprimen en una impresora también equipada con Bluetooth.
- PAN Profile –**P**ersonal **A**rea **N**etwork Profile- Perfil de Red de Área Personal. Describe como hasta siete dispositivos pueden interconectarse entre sí. Estableciendo automáticamente cual es el dispositivo master como describimos más arriba.
- Synchronization Profile – Perfil para sincronización de dispositivos de escritorio como PDA a PC, Teléfono celular a Notebook, ETC.

3.1.3 Dependencias de los Servicios de Bluetooth



Hasta el momento Bluetooth no es un estándar como lo es 802.11x en Wireless, Dentro del grupo PAN (Personal Area Networks) de la organización IEEE, está previsto adoptar rápidamente a Hand-helds como el estándar IEEE 802.15.

3.2 SEGURIDAD

Bluetooth tiene niveles de seguridad altos, por ejemplo encriptación de datos hasta 128 bits. El diseño de la seguridad en Bluetooth esta pensada para automatizar las tareas de reconocimiento y autenticación, hay tres posibilidades de seguridad establecidas en la norma. Pasemos a describirlas:

- **No seguro:** Este modo está pensado para la utilización pública de dispositivos Bluetooth, como por ejemplo el uso de una impresora donde un dispositivo establece una comunicación con la impresora descarga la impresión y se desconecta
- **Nivel de Seguridad Forzada a Servicios**: En este nivel la seguridad está limitada a la utilización de un servicio EJ: Un dispositivo puede tener permisos para descargar archivos a una PC pero no para tener acceso a la lista de contactos o a la agenda personal.
- **Nivel de Seguridad forzada a Enlace:** Es el nivel más alto de seguridad y requiere autenticación y autorización para poder establecer el vínculo Por EJ: Un teléfono celular que puede ser utilizado por un número limitado de personas.

Una vez establecido el nivel de seguridad los dispositivos deben pasar a la última etapa que es conocida como *apareamiento* (Pairing en Ingles) -También se hace referencia a este término como "*bonding*" Este concepto es introducido para que una vez establecida la comunicación entre los dos o más dispositivos se pongan de acuerdo en los niveles de encriptación y seguridad haciendo que un dispositivo que no esté *apareado* no pueda leer los datos transmitidos entre los dispositivos.

Dispositivos del mercado con soporte Bluetooth:

	
MSI PC2PC (USB)	Nokia 3600
	
PalmOne Zire 72	HP DeskJet 995ck
	
Optical Desktop For Bluetooth	Notebook Acer Ferrari 3000

4 WIRELESS

Es una tecnología que posibilita la conectividad entre PC's sin la utilización de cables mediante el uso de placas inalámbricas y antenas.

Esta tecnología de comunicación inalámbrica nos permite, la movilidad de los dispositivos al no estar conectado físicamente con un cable, unificar el acceso a las redes LAN con anchos de banda mas elevados, flexibilidad a la hora de implementación, sin generar cambios en la estructura edilicia alterando así la estética de los ambientes, facilidad de uso y operación, tiende a ser económica y reutilizable, ya que no esta sujeta a cables.

Dado el método de funcionamiento no es una tecnología que se destaque por su seguridad, aun los mecanismos diseñados no son lo suficientemente seguros para mantener a salvo la información, pero como contrapartida llegan a velocidades de comunicación bastantes sobresalientes.

Respecto a la tecnología de transmisión utiliza el mismo rango de frecuencia y banda ISM que Bluetooth, pero con un sistema de modulación de la señal distinto llamado DSSS y que trataremos mas adelante.

Escenarios de Implementación Wireless

- Edificios Históricos (Museos)
- Edificaciones con problemas estructurales
- Comercios (Pub's, Restaurantes, Bares)
- Complejos Residenciales
- Country's
- Casas y Departamentos
- Empresas (Oficinas)

4.1 ORGANIZACIONES Y ESTANDARES

4.1.1 Wi - Fi Alliance

WI - FI Alliance es un conjunto de fabricantes que tienen como objetivo el desarrollo y la implementación de las tecnologías inalámbricas, como así también el testeo de los dispositivos que salen al mercado. Fue fundada en 1999 y cuenta con más de 200 miembros, algunos de ellos son marcas prestigiosas que llevaron desde el comienzo este proyecto, ellas son: Agere, Cisco, Conexant, Dell, Intel, Microsoft, Nokia, Philips, Sony, Symbol Technologies y Texas Instruments.

4.1.2 IEEE

IEEE (The Institute of Electrical and Electronics Engineers) es una sociedad mundial que agrupa a técnicos y científicos con el fin de fomentar la innovación tecnológica, y contribuir con el desarrollo profesional de sus miembros.

Es la encargada de desarrollar y establecer los estándares de fabricación de dispositivos electrónicos. Ahora bien, tenemos que definir a estándar, según la IEEE es una publicación en donde se establece por consenso y aprobación de los miembros de esta organización, el conjunto de procedimientos y especificaciones que asegure que cualquier material, producto, método o servicio funcione a los propósitos para los cuales fueron creados.

Dentro de las redes Wireless existen diversos estándares de fabricación (calificados por la IEEE) que nos permiten por sus características tener diferentes anchos de banda, distintos métodos de seguridad y mejorados mecanismos de comunicación.

Cabe destacar que también existen sistemas propietarios los cuales ofrecen otros tipos de ancho de banda que no son compatibles con los estándares de la IEEE, así que debemos prestar mas que atención al momento de implementar una WLAN en la compra de las NIC's. Por ejemplo las NIC's Planet Wire Free soportan 22 Mbps como estándar y por lo tanto no pueden establecer una comunicación con una placa de 54 Mbps.

A continuación una tabla con los protocolos estandarizados por la IEEE

Protocolo de comunicación (capa física)	**Ancho de banda**	**Frecuencia de operación**
IEEE 802.11	1 y 2 Mbps	2.4 Ghz
IEEE 802.11b	11 Mbps	2.4 Ghz
IEEE 802.11g	54 Mbps	2.4 Ghz
IEEE 802.11a	54 Mbps	5 Ghz

Extensiones de estándares	Tipo de servicio
IEEE 802.11d	Permite a los Access Point comunicar información sobre el canal disponible y la potencia máxima admisible para realizar un enlace.
IEEE 802.11e	Permite implementar calidad de servicio QoS, su finalidad es la priorización del tráfico en base al tipo de información.
IEEE 802.11f	Lograr la interoperatividad entre Access Point de distintos fabricantes para realizar Roaming.
IEEE 802.11h	Control de potencia admisible y selección de frecuencia automática para la banda de 5 GHz.
IEEE 802.11i	Implementación de seguridad mejoradaza WPA. Hoy implementado sobre 802.11g.

En la primera tabla los datos que tenemos disponibles son los correspondientes al medio de transporte utilizado para llevar a cabo la conexión que se especifican en la norma emitida por el IEEE, dentro de los cuales el más sobresaliente es la frecuencia de trabajo del sistema, ya que es la más relevante al momento de adquirir un dispositivo.

La segunda tabla es una colección de estándares que proveen de servicios adicionales a los expuestos en la primera, en este punto se debe destacar que la promoción de un nuevo servicio por un fabricante debe estar acompañado por una leyenda en la cual declare el cumplimiento de la misma, de lo contrario pude ser considerada como propietaria.

4.2 FUNCIONES EN LA CAPA FÍSICA

Igual que en una red cableada esta capa específica las técnicas de cómo viajarán la señales, en este caso el tipo de ***modulación*** y el ***número de canal*** a utilizar.

La modulación mas utilizada es la **DSSS** (Direct Sequence Spread Spectrum - Espectro Extendido de Secuencia Directa) y los canales disponibles para transmitir son 11 dependiendo de las reglamentaciones vigentes en cada país.

4.3 FUNCIONES DE LA CAPA DE ENLACE

Wireless al igual que cualquier otro sistema de transmisión, requiere de un protocolo de comunicación para poder acceder al medio (el canal por donde se transmite) y los mecanismos que prevengan la superposición y monopolización del mismo por parte de las estaciones.

Esta tecnología del acceso al medio se la denomina **CSMA / CA** (Carrier Sense Multiple Access with Collision Avoidance) muy similar a la estudiada en la redes Ethernet ya que se sigue detectando una portadora (escuchando el medio antes de hablar), todos compiten por ingresar al mismo y finalmente sobreviene la diferencia ya que en este caso no se detectan las colisiones si que se las evita (CA Collision Avoidance – Evitación de Colisiones).

Una de las explicaciones del porque se tienen que evitar las colisiones, es debido al sistema que se implementa en la transmisión y recepción dificulta la detección de la portadora (no se escucha correctamente siempre) dependiendo de los materiales del entorno y posición de los dispositivos.

La segunda razón es mas sencilla, ya que la única antena que posee una placa de red Wireless sirve tanto para transmitir como para recibir una señal, y por lo tanto no puede realizar estas dos tareas al mismo tiempo (transmitir y escuchar lo que transmite para detectar una colisión).

Este es solo el principio básico de funcionamiento del protocolo como solución a un problema puntual, pero también debemos decir que existen otros obstáculos y por supuesto el paliativo correspondiente a cada uno de ellos.

4.4 MODOS DE COMUNICACIONES.

Existen dos modalidades de comunicación en las redes inalámbricas, una nos permite la comunicación punto a punto (Ad-Hoc) o sea de PC a PC, y otra modalidad nos permite poder unirnos a una red cableada mediante un punto de acceso conocido como Access Point.

4.4.1 Ad-Hoc

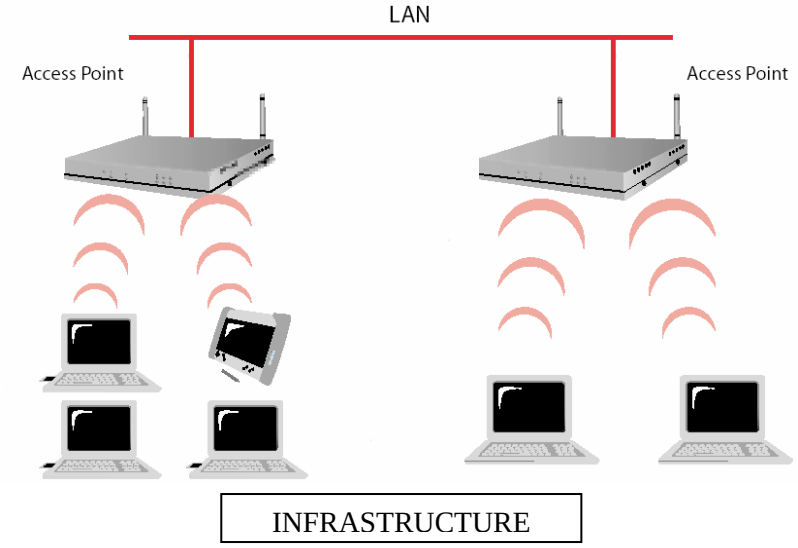
Modo de comunicación en una red Wireless donde se omite la utilización de un Access Point para enlazar una red física con una red inalámbrica.

La comunicación se establece punto a punto entre las estaciones de trabajo, sin acceder a un repetidor, utilizando únicamente las placas de red wireless.

AD-HOC

4.4.2 Infrastructure

Este modo de comunicación se utiliza para enlazar una LAN con una red inalámbrica (WLAN), utilizando como medio de enlace un dispositivo denominado Access Point (punto de acceso). Este permite que las estaciones de trabajo que no estén conectadas a una LAN, puedan hacerlo mediante un enlace inalámbrico (placa de red Wireless) y viceversa.



INFRASTRUCTURE

Adaptadores de Red Wireless

La función del adaptador de red (NIC) es aceptar datos del sistema operativo, (paquetes de red generados por el protocolo IP en nuestro caso), marcarlos para su seguimiento, y haciendo uso de un protocolo de enlace de datos y acceso al medio (IEEE 802.11) introducirlo en un medio de transmisión (ondas electromagnéticas de radiofrecuencia capaces de propagarse en el vacío para nosotros). El proceso inverso (entregar al sistema operativo datos captados del medio de transmisión) también está a cargo de un NIC.

Los diversos adaptadores de red tienen distintas características que es necesario conocer a la hora de adquirir uno de ellos:

- *Interfaz:* Indica si el dispositivo se conecta a una ranura PCI, ISA o PCMCIA.

- *Chipset:* Es el circuito integrado que contiene la electrónica del dispositivo. Es importante conocerlo para saber si existe un driver que podamos usar en nuestro sistema operativo para manejar al dispositivo.
- *Versión de la norma 802.11 que soporta:* Determina entre otras cosas la funcionalidad disponible y las tasas de bits de transmisión que se pueden utilizar. Las versiones de la norma son retro compatibles. Así, una placa más nueva, capaz de operar a 11 Mbps, puede comunicarse con otra placa de 2 Mbps (a 2 Mbps, obviamente).
- *Capacidad de actualizar el firmware:* Si el software embebido en el dispositivo (firmware) está almacenado en una memoria flash, es posible sobre escribirlo con una versión más nueva que soporte más funciones o tenga menos errores.

4.5 PROPAGACIÓN DE LA SEÑAL

Las construcciones (casas, edificios, oficinas) pueden impactar de manera dramática en la calidad de la señal de una WLAN.

La madera, el metal y otros tipos de materiales tienen un impacto directo sobre la propagación y la absorción de la señal. Otros factores pueden ser:

- Interferencias de múltiples orígenes: Ocurre cuando la longitud y tiempo de la señal son reflectadas por muros, paredes, armarios de metal, rayos y otros objetos, esto hace que un mismo dispositivo reciba dos o mas señales idénticas. Este efecto también es conocido localmente como fantasma.
- Fading: es la reducción de la señal cuando esta va atravesando paredes y techos.
- Zonas Muertas (Dead Zones): Son lugares donde el radio de señal nunca se alcanza debido a reflexiones, obstrucciones u otras condiciones ambientales.

Son muchas las variantes de interferencias que existen a nuestro alrededor, las tecnologías Wireless pueden minimizar estas interferencias pero nunca superarlas.

4.5.1 Tipo de Antenas:

Generalmente en 802.11x se pueden utilizar dos clases de antenas, direccionales y omnidireccionales.

Las antenas omnidireccionales poseen la característica de transmitir en un ángulo de 360º y son capaces de recibir señales desde cualquier ubicación.

En cambio las antenas direccionales concentran la energía de las señales enviadas y recibidas de forma similar al reflector de una linterna.

Un buen ejemplo de esta tecnología es la antena en forma de parábola, ya que solo puede recibir la señal desde su lado cóncavo, este a su vez que actúa como concentrador de todas las señales que se reflejan en su superficie y se dirigen al elemento receptor propiamente dicho ubicado en el centro de la antena.

El tipo de antena a utilizar, su ubicación y diversos factores tanto ambientales como edilicios, juegan un papel importante a la hora de montar una WLAN.

A continuación podremos observar tres tipos de antenas destinadas para largo alcance en comunicaciones Wireless dentro del rango de frecuencia que va desde los 2300 a 2500 MHz, que permiten la instalación de sistemas punto a punto y punto a multipunto.

En la Fig. 1 se observa una antena Omnidireccional de exteriores (esta se encuentra miniaturizada por razones de espacio) y al lado de esta se encuentra una antena omnidireccional de las que se proveen con la NIC Wireless, el la Fig 2 una del tipo Yagui, y en la Fig. 3 una Antena Parabólica, estas dos ultimas cumplen con distintos objetivos al momento del enlace.

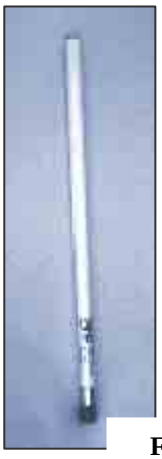


Fig. 1

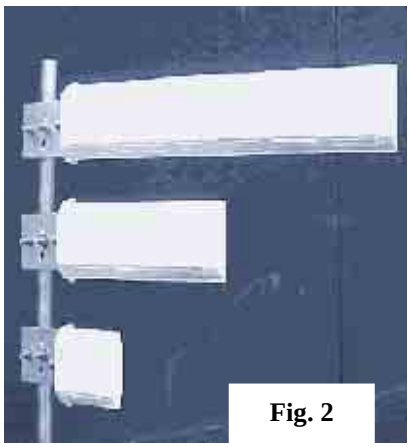


Fig. 2

Fig. 3

4.6 SEGURIDAD EN WIRELESS

La seguridad de una red es un punto clave, tengamos en cuenta que en una LAN privada el acceso queda a cargo de un administrador que puede o no otorgarnos la posibilidad de acceder a ella, en cambio en una WLAN la seguridad juega un papel mas importante, ya que las transmisiones se hacen en un medio (aire) donde pueden ser captadas por otros dispositivos que utilicen la misma tecnología inalámbrica poniendo en riesgo la confidencialidad de los datos de los usuarios.

- **WEP: Wireless Equivalent Privacy**, es un mecanismo de encriptación de datos que utiliza 64 o 128 bits y fue diseñado para el estándar 802.11b. Todos los dispositivos que cumplen este estándar tienen la posibilidad de habilitar este mecanismo de encriptado de datos, funciona proporcionando una contraseña la cual debe respetar ciertos caracteres y longitudes para poder iniciar una comunicación segura, no es una contraseña para validarse como usuario, sino que es una validación entre estaciones para empezar a transmitir datos de forma segura.

- **Modos OSA y SKA (abierto o compartido)**, estas dos modalidades permiten establecer la seguridad al momento de la conexión, una red del tipo Abierta (OSA – Open System Authentication) puede ser vista y accedida por cualquier usuario que este dentro del área de señal, sin tener que validar la estación de trabajo emisora contra la receptora. El modo Compartido (SKA – Shared Key Authentication) debe validarse mediante una contraseña que es enviada desde la estación emisora hacia la receptora con el fin de poder entablar una comunicación.

4.7 WI-FI HOTSPOTS

Los Hotspots o también conocidas como Islas de Conectividad, son nada menos que lugares donde se brinda de forma gratuita o no, conexión a redes publicas mediante Wireless.

Como un elemento de moda y de valor agregado, se esta empezando a brindar a los clientes en bares, restaurantes, estaciones de servicio y hoteles la posibilidad de acceder a Internet si se cuenta con un equipo portátil, ya sea Notebooks o PDA's con tecnología Wireless.

Telecom ha desplegado una red "al aire libre" sobre todo Puerto Madero, también coloco en el Aeroparque metropolitano y en el Aeropuerto de Ezeiza Hotspots para que pasajeros puedan conectarse entre las esperas de embarque.

NOTAS

CUESTIONARIO CAPITULO 6

1.- En Wireless ¿Cual es la diferencia entre una red Infrastructure y una Ad Hoc?

2.- ¿Implementaría una red Wireless como solución integral en un ambiente empresarial?

3.- ¿Como seleccionaría una placa Wireless que debe ser integrarla a una red Wireless ya existente?

4.- ¿Que debería tener en cuenta cuando tenga que diseñar y presupuestar una red Wireless?