Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

Comparación entre las tecnologías de conexión inalámbricas

Bluethoo y Wi-Fi

Trabajo de graduación previo a la obtención del título de Ingeniero de Sistemas

Autores: Ávila Duran Esteban
Guzmán Espadero Wilson

Director: Ing. Bolívar Méndez Rengel

Cuenca, Ecuador

2006

DEDICATORIA

Este trabajo monográfico esta dedicado a mis padres, hermanos y aquellas personas que me brindaron su apoyo incondicional para la elaboración y culminación de este documento.

AGRADECIMIENTO

Expresamos nuestros mas sinceros agradecimientos a todos los profesores que nos han brindado sus conocimientos, ya que sin estos no hubiera sido posible la realización de esta monografía, especialmente al Ing. Bolívar Méndez que nos ha dirigido de una forma muy acertada permitiéndonos así, terminar con éxito y excelencia.

INDICE DE CONTENIDOS

RESUMEN

COMPARACIÓN DE LAS TECNOLOGÍAS DE CONEXIÓN INALÁMBRICAS BLUETOOTH Y WI-FI

La presente monografía va dirigida a todos aquellos estudiantes y profesionales que necesiten una referencia acerca de las tecnologías de comunicación inalámbrica, como son: Bluetooth y Wi-Fi. Aborda los aspectos más relevantes y de actualidad en el mundo de las comunicaciones, no con gran profundidad ya que ello resulta imposible por la gran cantidad de tecnologías existentes, pero sí con los conceptos que son imprescindibles para tener un conocimiento básico de los temas tratados.

En el primer lugar se describe una breve introducción de los aspectos básicos de la tecnología inalámbrica como son: concepto, datos más importantes de la tecnología, Radio Comunicación, Antenas y Transmisión RF. Luego se trata de temas elementales como seguridad, topología, etc., de las tecnologías Bluetooth y Wi-Fi. Finalmente, se presenta un estudio a cerca del funcionamiento de estas dos tecnologías y luego la instalación y configuración del hardware y software utilizados para las pruebas de transmisión de datos.

En el mundo actual, las comunicaciones entre dispositivos electrónicos es una necesidad tecnológica básica, en particular, los dispositivos que se encuentran a corta distancia y que normalmente se comunican entre si por medios alambrados. Estos utilizan una amplia gama de cables y conectores que hacen la comunicación, en un momento dado, limitada, falible e incomoda en situaciones donde existen demasiados cables. Las tecnologías Wi-Fi dentro del estándar IEEE 802.11 y Bluetooth permiten realizar la comunicación entre dispositivos de forma más dinámica y sencilla entre dispositivos cercanos.

La monografía incluye un glosario de palabras claves utilizadas en este documento, una lista de direcciones útiles de Internet, donde se encontrará información adicional para aquellos lectores interesados en ampliar conocimientos sobre el tema.

ABSTRACT

COMPARISON OF THE WIRELESS CONNECTION TECHNOLOGIES BLUETOOTH AND WI-FI

The present research work is addressed to all those student and professionals who need reference about wireless communication technologies such as Bluetooth and Wi-Fi. It focuses on the most relevant and up-dated aspects in the communication word, although, not very deeply since that would be impossible due to the great amount of existent technologies. However, it offers the concepts that are indispensable to have a basic knowledge of the topics under study.

It begins with a brief introduction where the basic aspect of wireless technology, such as the concept, the most important technology data, radio communication, antennas, and RF transmission are described. The some elementary topics as safety, topology, etc. regarding Bluetooth and Wi-Fi technologies are discussed. Finally, a study about the operation of these two technologies is presented, followed by the installation and configuration of the hardware and software used for the data transmission tests.

In the present word, communication through electronic devices is a basic technological need, particularly between devices that are located at a short distance and normally communicate with each other through wired means. These use a wide range of cables and connectors which limit communication, turning it fallible and uncomfortable in situations where there are too many cables. Both technologies, Wi-Fi within the standard IEEE 802.11 and Bluetooth make it possible to establish communication between devices in a more dynamic and simple way when they are near.

The research work includes a glossary of the key-words used in this document as well as a useful Internet address list whit additional information for those readers interested in extending their knowledge about the subject.

CAPITULO I

INTRODUCCIÓN A REDES INALÁMBRICAS

1.1. Introducción

Las redes inalámbricas son una tecnología que ha ganado muchos usuarios, puesto que sigue creciendo tanto en velocidad como en cobertura.

Lo que busca la tecnología inalámbrica es suprimir al mínimo el cableado estructurado. Convirtiendo a las redes actuales mas estéticas y con fácil movilización de los equipos.

Esta es una tecnología que se ha venido utilizando en lugares en los que se complica la conexión mediante cables y de difícil acceso.

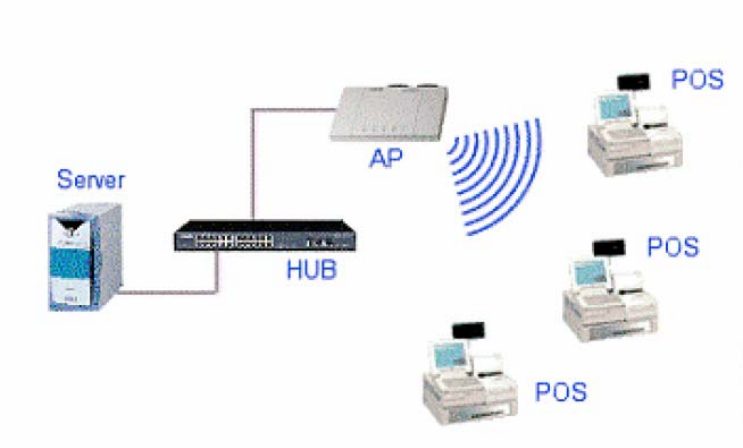
Las tecnologías que se describen este trabajo de graduación son Bluetooth y *Wi-Fi*, que trabajan en la banda libre de 2,4Ghz en los países de América, pero con ciertas restricciones en algunos países de Europa.

Al ser dispositivos inalámbricos se debe tener en cuenta los tipos de seguridades que estos poseen, por lo que se realizará una investigación sobre los mecanismos usados para proteger nuestra información, ya que en la actualidad se ha convertido en un activo más de las empresas.

Lo que se espera obtener con el desarrollo de nuestra monografía es un conocimiento del funcionamiento de las tecnologías *Wi-Fi* y Bluetooth en diferentes ambientes.

1.2. Concepto:

Wireless es una tecnología que permite comunicar computadoras mediante Ondas de Radio o Luz Infrarroja. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en diferentes ambientes.



[1]Figura 1 Ilustración de red inalámbrica

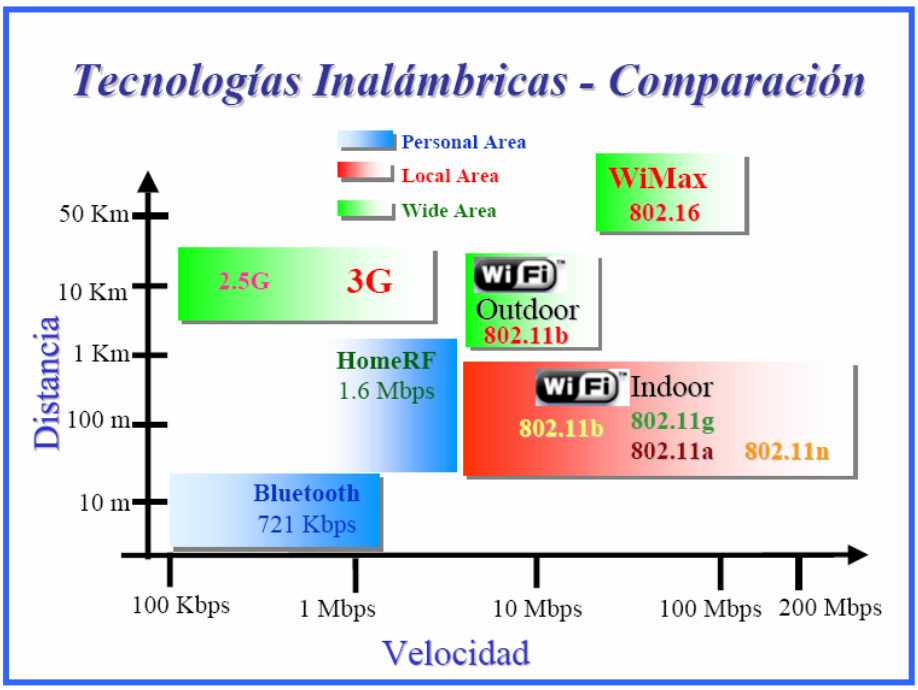
Existen dos amplias categorías de Redes Inalámbricas:

- De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países vecinos (mejor conocido como Redes de Área Metropolitana *MAN*).
- De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas, cuyas oficinas se encuentran en uno o varios edificios aledaños.

1.3. Datos más importantes:

La tecnología inalámbrica revolucionó la vida de los usuarios permitiendo conectarse directamente con las personas y la información relevante mediante una conexión a alta velocidad desde cualquier parte. INTEL asume que las tecnologías inalámbricas como *3G, Wi-Fi, WiMAX y UWB* coexistirán funcionando de forma sinergética para cubrir las necesidades de los usuarios.

[1] Ing. Martín Vernengo, mvernel@fi.uba.ar Curso Argentina Wlan



[2]Figura 2: Comparación de Tecnologías inalámbricas

1.3.1. *Wimax*

Las redes metropolitanas inalámbricas (*WMAN*) cubren una distancia mucho mayor que las *WLAN*, interconectando edificios entre sí dentro de una amplia área geográfica. La nueva tecnología *WiMAX* (802.16d hoy día y 802.16e en un futuro próximo) permitirán mayor movilidad y reducirán la dependencia de las conexiones con cable.

1.3.2. *Wi-Fi*

Las redes locales inalámbricas (*WLAN*) disponen de un alcance más amplio que las *WPAN*, normalmente se ubican en edificios de oficinas, restaurantes, tiendas, casas, etc. Las *WLAN* van ganando popularidad, alimentada en parte por la disponibilidad de dispositivos optimizados para la informática inalámbrica como la tecnología móvil INTEL Centrino.

[2] Ing. Martín Vernengo, mvernel@fi.uba.ar Curso Argentina Wlan

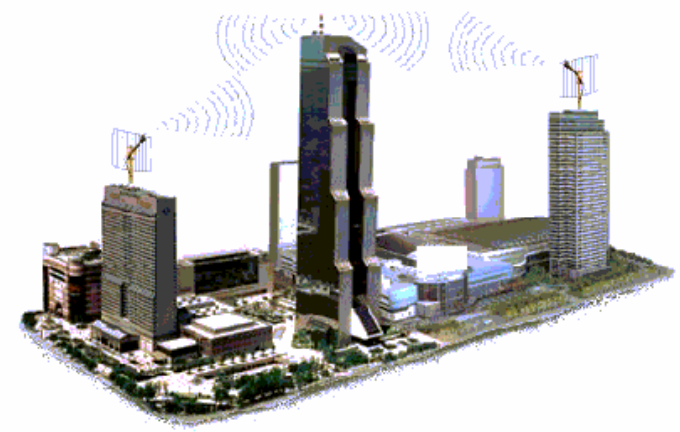
1.3.3. 3G

Redes amplias inalámbricas (*WWAN*) son redes inalámbricas de mayor alcance, así como las más utilizadas hoy día en la infraestructura de telefonía móvil, aunque también disponen de la capacidad de transmitir datos. Los servicios de próxima generación de telefonía móvil basados en las diversas tecnologías *3G* mejorarán significativamente las comunicaciones *WWAN*.

1.4. Conceptos generales.

1.4.1. Radio Comunicación.

La radio comunicación es una tecnología que posibilita la transmisión de señales mediante la modulación de ondas electromagnéticas. Éstas son ondas que pueden propagarse tanto a través del aire como del espacio vacío y no requieren un medio de transporte.



[3]Figura 3: Ilustración de Radio Enlace

Una onda de radio se origina cuando una partícula cargada (por ejemplo, un electrón) se excita a una frecuencia situada en la zona de radiofrecuencia (RF) del espectro electromagnético.

[3] Ing. Martín Vernengo, mvernel@fi.uba.ar Curso Argentina Wlan

Cuando la onda de radio actúa sobre un conductor eléctrico (la antena), induce en él un movimiento de la carga eléctrica (corriente eléctrica) que puede ser transformado en señales de audio u otro tipo de señales portadoras de información.

Aunque empleamos la palabra radio, las transmisiones de televisión, radio, radar y telefonía móvil están incluidos en esta clase de emisiones de radiofrecuencia.

1.4.2. Que es una antena?

Figura 4: Ilustración de Antenas

Es un dispositivo capaz de emitir o recibir ondas de radio. Está constituida por un conjunto de conductores diseñados para radiar (transmitir) un campo electromagnético cuando se le aplica una fuerza electromotriz alterna.

De manera inversa, en recepción, si una antena se coloca en un campo electromagnético, genera como respuesta a éste una fuerza electromotriz alterna.

El tamaño de las antenas está relacionado con la longitud de onda de la señal de radiofrecuencia transmitida o recibida, debiendo ser, en general, un múltiplo o submúltiplo exacto de esta longitud de onda. Por eso, a medida que se van utilizando frecuencias mayores, las antenas disminuyen su tamaño.

Asimismo, dependiendo de su forma y orientación, pueden captar diferentes frecuencias, así como niveles de intensidad.

1.4.3. Transmisión por Radiofrecuencia.

En este caso se trata de transmisión de datos y audio a través de ondas de radio. El sistema consta de bases de transmisión de radio frecuencia que emiten una señal de FM (frecuencia modulada) que es captada por el receptor. No es necesario la línea de vista entre los equipos. Funciona perfectamente tanto en espacios cerrados como al aire libre.

CAPITULO II

WI - FI

2.1. Que es Wi-Fi?

Figura 5: Componentes de una red *WI-Fi*

El protocolo *IEEE 802.11* o *WI-FI* es un estándar de protocolo de comunicaciones de la *IEEE (The Institute of Electrical and Electronics Engineers)* que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una *WLAN*. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia *802.11* actualmente incluye seis técnicas de transmisión por modulación que utilizan los mismos protocolos. El estándar original de este protocolo data de 1997, era el *IEEE 802.11*, tenía velocidades de 1 hasta 2 *Mbps* y trabajaba en la banda de frecuencia de 2,4 *GHz*. En la actualidad no se fabrican productos en base a este estándar. El término *IEEE 802.11* se utiliza también para referirse a este protocolo al que ahora se conoce como "*802.11* legacy." La siguiente modificación apareció en 1999 y es designada como *IEEE 802.11b*, esta especificación tiene velocidades de 5 hasta 11 *Mbps*, a una frecuencia de 2,4 *GHz*. También se realizó una especificación sobre una frecuencia de 5 *Ghz* que alcanzaba los 54 *Mbps*, era la *802.11*ª y resultaba incompatible

con los productos de la *802.11*b y por motivos técnicos casi no se desarrollaron productos.

Posteriormente se incorporó un estándar a esa velocidad y compatible con el *802.11*b que recibiría el nombre de *802.11*g. En la actualidad la mayoría de productos son de la especificación *802.11*b y de la *802.11*g (Actualmente se está desarrollando la *802.11*n, que se espera que alcance los 500 *Mbps*). La seguridad forma parte del protocolo desde el principio y fue mejorada en la versión *802.11*i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el *802.11*b. En el 2005, la mayoría de los productos que se comercializan adoptan el estándar *802.11*g con compatibilidad hacia el *802.11*b.

Los estándares *802.11*b y *802.11*g utilizan bandas de 2,4 *Ghz* que son de libre uso. El estándar *802.11*ª utiliza la banda de 5 *GHz*. Las redes que trabajan bajo los estándares *802.11*b y *802.11*g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4 *Ghz*.

2.2. Seguridad En *Wi-Fi, 802.11*

Los tres aspectos fundamentales que se deben tener en cuenta al diferenciar una red *Wi-Fi* de una cableada, son:

- Autenticación
- Control de acceso
- Confidencialidad

2.2.1. Autenticación y control de acceso:

Los métodos que se emplean son los siguientes:

- *SSID* (Service Set Identifier): Contraseña (*WEP*).
- Seguridad por restricción de direccionamiento *MAC*: Permite restringir a un listado de direcciones, las que se pueden conectar y las que no.
- Contraseñas no estáticas:

- Periódicas
- *OTP (One Time Password):* Contraseñas de un solo uso, también conocidas como token flexibles.

2.2.2. *WEP*

WEP (*Wired Equivalent Privacy*, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma *IEEE 802.11*. Los objetivos de *WEP*, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes *WLAN*.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es *RC4* con claves (*seed*), según el estándar, de 64 *bits*. Estos 64 *bits* están formados por 24 *bits* correspondientes al vector de inicialización más 40 *bits* de la clave secreta. Los 40 *bits* son los que se deben distribuir manualmente. El vector de inicialización (*IV*), en cambio, es generado dinámicamente y debería ser diferente para cada trama.

El objetivo perseguido con el *IV* es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave.

2.2.3. WPA

WPA (Wi-Fi Protected Access, acceso protegido *Wi-Fi*) es la respuesta de la asociación de empresas *Wi-Fi* a la seguridad que demandan los usuarios y que *WEP* no puede proporcionar.

El *IEEE* tiene casi terminados la implementación de un nuevo estándar para reemplazar a *WEP*, que se publicarán en la norma *IEEE 802.11*i. Debido al atraso (*WEP* es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), la *IEEE* decidió que *Wi-Fi*, tome aquellas partes del futuro estándar que ya estaba suficientemente desarrollado y publicar así el *WPA* que es un subconjunto de lo que se llama *IEEE 802.11*i, el mismo que se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de *WEP* y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan *WPA*, no consideren la necesidad de cambiar a *IEEE 802.11*i, cuando esté disponible.

2.2.3.1. Características de *WPA*

Las principales características de *WPA* son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- *IEEE* 802.1X. Estándar del *IEEE* de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo *EAP* y un servidor *AAA (Authentication Authorization Accounting)* como puede ser *RADIUS* (*Remote Authentication Dial-In User Service*). Si la autorización es positiva, entonces en el punto de acceso se permite abrir el puerto. El servidor *RADIUS* puede contener políticas para ese usuario concreto, que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

- *EAP:* definido en la *RFC 2284*, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y confiabilidad. *EAP* fue diseñado originalmente para el protocolo *PPP (Point-to-Point Protocol)*, aunque *WPA* lo utiliza entre la estación y el servidor *RADIUS*. Esta forma de encapsulación de *EAP* está definida en el estándar 802.1X bajo el nombre de *EAPOL (EAP over LAN)*.
- *TKIP (Temporal Key Integrity Protocol)*. Según indica *Wi-Fi*, es el protocolo encargado de la generación de la clave para cada trama.
- *MIC (Message Integrity Code)*. Código que verifica la integridad de los datos de las tramas.

2.2.3.2. Modos de funcionamiento de *WPA*

WPA puede funcionar en dos modos:

- Con servidor *AAA, RADIUS* normalmente: Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y confiabilidad.
- Con clave inicial compartida (*PSK*): Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor *AAA*, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en *WEP*, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.2.4. *WPA2* (*IEEE 802.11i*)

*802.11*i es el nuevo estándar del *IEEE* para proporcionar seguridad en redes *WLAN*. *Wi-Fi* está haciendo una implementación completa del estándar en la especificación *WPA2*.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado *AES (Advanced Encryption Standard)*, desarrollado por el *NIS*. Se trata de un algoritmo de cifrado de bloque (*RC4* es de flujo)

con claves de 128 *bits*. Requerirá un *hardware* potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar *WPA2*.

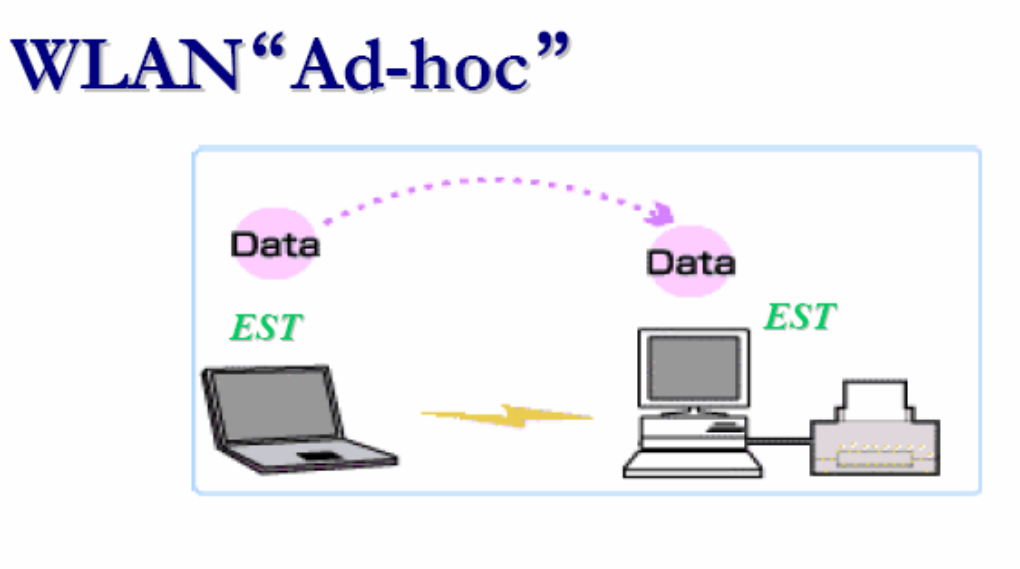
Para el aseguramiento de la integridad y autenticidad de los mensajes, *WPA2* utiliza *CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol)* en lugar de los códigos *MIC*.

Otra mejora respecto a *WPA* es que *WPA*2 incluirá soporte no sólo para el modo *BSS* sino también para el modo *IBSS* (redes ad-hoc).

2.3. Topología *Wi-Fi*

El estándar *IEEE 802.11* presenta dos topologías:

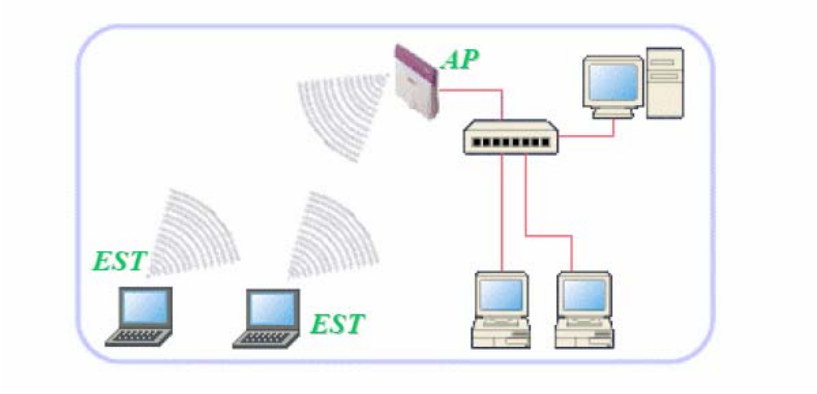
- *Ad Hoc (o peer to peer)*: Dos o más clientes que son iguales entre ellos.



[4]Figura 6: Topología Ad-hoc

[4] Ing. Martín Vernengo, mvernel@fi.uba.ar Curso Argentina Wlan

- Infraestructura: Red centralizada a través de uno o más *Access Point* (*AP*).



[5]Figura 7: Topología Infraestructura

Descripción general de componentes de las mismas:

- *BSS (Basic Service Set):* Es el bloque básico de construcción de una *LAN 802.11*. En el caso de tratarse de únicamente 2 estaciones ser denomina *IBSS (Independent BSS)*, es lo que a menudo se denomina "*Ad Hoc Netwok*".
- *DS (Distribution System):* Es la arquitectura que se propone para interconectar distintos *BSS*. El *AP* es el encargado de proveer acceso al *DS*, todos los datos que se mueven entre BSS y DS se hacen a través de estos *AP*, como los mismos son también *STA*, son por lo tanto entidades direccionables.
- ESS (Extended Service Set): Tanto BSS como DS permiten crear *wireless network* de tamaño arbitrario, este tipo de redes se denominan redes ESS.
- La integración entre una red *802.11* y una No *802.11* se realiza mediante un Portal. Es posible que un mismo dispositivo cumpla las funciones de *AP* y Portal.

[5] Ing. Martín Vernengo, mvernel@fi.uba.ar Curso Argentina Wlan

2.3.1. Modelo de Capas de *Wi-Fi*

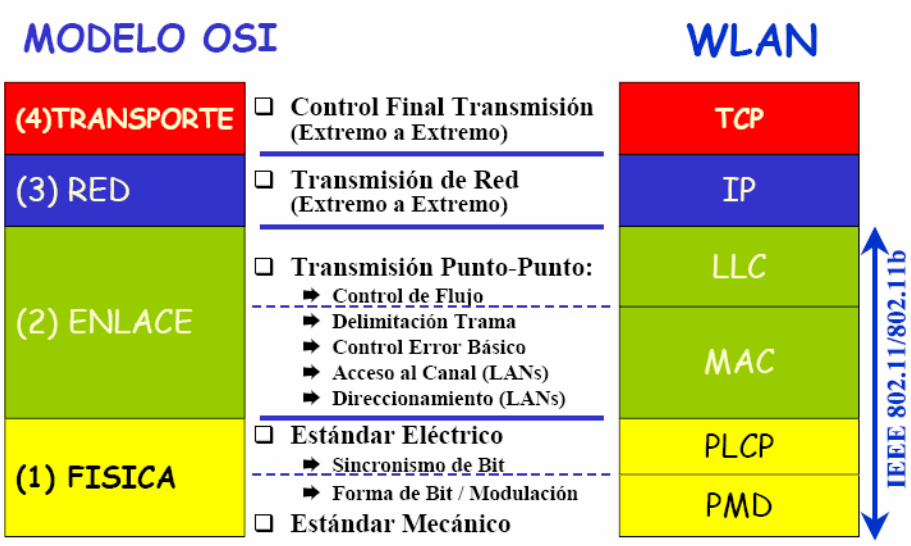


Figura 8: Modelo de capas *Wi-Fi*

2.3.1.1. La capa física de *802.11*:

La capa física la componen dos subcapas: *-PLCP (Physical Layer Convergence Protocol)*: Se encarga de codificación y modulación.

- Preámbulo (144 *bits* = 128 sincronismo + 16 inicio trama).
- *HEC (Header Error Control): CRC 32*
- Modulación (propagación) *DSSS o FHSS o IR.*
- *PMD (Physical Medium Dependence):* Es la que crea la interfaz y controla la comunicación hacia la capa *MAC* (a través del *SAP: Service Access Point*)

Este nivel lo conforman dos elementos principales:

- Radio: Recibe y genera la señal.
- Antena: Recibe y transmite las señales, existiendo varios tipos para cada aplicación.

Hay algunos aspectos físicos que vale la pena profundizar para la comprensión de *Wi-Fi*, de los cuales se recomienda especialmente:

- *FHSS (Frequency Hopping Spread Spectrum*) para la banda de 2,4 *GHz (ISM: Industrial, Scientific and Medical band.*

- *DSSS (Direct Sequence Spread Spectrum* para 2,4 *GHz*.
- *IR (InfraRed).*

NOTA: Aunque esto no forma parte de los conceptos de *Wi-Fi*, cuando se habla de transmisión, se deben diferenciar tres términos:

- Modulación: Es el método de emplear una señal portadora y una moduladora (que da forma a la anterior). Cada una de ellas puede ser analógica o digital, con lo cual se obtienen cuatro posibles combinaciones de portadora y moduladora *(AA – AD – DA y DD),* con las cuales se conforman todas las técnicas de modulación. *Wi-Fi* en la mayoría de los casos emplea la técnica *QAM* Modulación de Amplitud en Cuadratura, es una forma de modulación digital en donde la información digital esta contenida, tanto en la amplitud como en la fase de la portadora transmitida. Por ejemplo 8QAM es una técnica de codificación M-ario en donde M = 8.
- Propagación: Es la forma en la cual "van saliendo" las señales al aire. Aquí es donde verdaderamente se aplican las técnicas de *DHSS y FHSS. SS (Spread Spectrum)* es la técnica de emplear muchas subportadoras de muy baja potencia con lo cual se "expande" el espectro útil. En cuanto a *DH y FH.* El ejemplo típico que se emplea para estas técnicas es la analogía con una Terminal de trenes, en la cual existen varios andenes. Para *DH,* los trenes estarían saliendo, primero el andén 1, luego el 2, a continuación el 3, 4, 5... y así sucesivamente, respetando siempre este orden. Para *FH,* la salida de los trenes no respeta el orden y puede ser aleatoria o acorde a un patrón determinado (*Wi-Fi* hace un muy buen uso de esto, pues en las subportadoras que recibe mucha interferencia no las usa o emplea menos cantidad de *bits* en las mismas).
- Codificación: Es la asociación de *bit* a cada "muestra" que se obtiene. *Wi-Fi* en la mayoría de los casos emplea el código *Barrer*, que está formada por 11 bits que tiene propiedades matemáticas que lo hacen ideal para modular radiofrecuencias. El código Barker genera series de objetos de datos llamados chips. Cada bit se codifica por el Código Barker de 11bits y cada grupo de 11 chips codifica 1 bit de datos.

2.3.1.2. La capa de enlace de *802.11*

Respetando el modelo OSI, en este contexto se asociara en el nivel de enlace, los dos subniveles que lo conforman (*MAC: Medium Access Control y LLC: Logical Link Control)*. Desde el punto de vista de *802.11*, solo interesa hacer referencia al subnivel *MAC*.

Capa *MAC*: Controla el flujo de paquetes entre 2 o más puntos de una red. Emplea *CSMA/CA: Carrier Sense Multiple Access / Collision avoidance*. Sus funciones principales son:

- Exploración: Envío de *Beacons* que incluyen los *SSID: Service Set identifiers* o también llamados *ESSID (Extended SSID*), máximo 32 caracteres.

- Autenticación: Proceso previo a la asociación. Existen dos tipos:
    - Autenticación de sistema abierto: Obligatoria en *802.11*, se realiza cuando el cliente envía una solicitud de autenticación con su *SSID* a un *AP*, el cual autorizará o no. Este método aunque es totalmente inseguro, no puede ser dejado de lado, pues uno de los puntos más fuertes de *Wi-Fi* es la posibilidad de conectarse desde sitios públicos anónimamente (terminales terrestres, hoteles, aeropuertos, etc.).
    - Autenticación de clave compartida: Es el fundamento del protocolo *WEP* (hoy totalmente desacreditado), se trata de un envío de interrogatorio (desafío) por parte del *AP* al cliente.

- Asociación: Este proceso es el que le dará acceso a la red y solo puede ser llevado a cabo una vez autenticado
- Seguridad: Mediante *WEP*, con este protocolo se cifran los datos pero no los encabezados.
- *RTS/CTS*: Funciona igual que en el puerto serie (*RS-232*), el aspecto más importante es cuando existen "nodos ocultos", pues a diferencia de *Ethernet*, en esta topología SÍ pueden existir nodos que no se escuchen entre sí y que solo lleguen hasta el *AP*, (Ej.: su potencia está limitada, posee un obstáculo entre ellos, etc.), en estos casos se puede configurar el empleo de *RTS/CTS*. Otro

empleo importante es para designar el tamaño máximo de trama (en *802.11* Es: mínimo=256 y máximo=2312 *Bytes*).

- Modo ahorro de energía: Cuando esta activado este modo, el cliente envió previamente al *AP* una trama indicando "que se irá a dormir", El *AP*, coloca en su buffer estos datos. Se debe tener en cuenta que por defecto este modo suele estar inactivo (lo que se denomina *Constant Awake Mode: CAM*).
- Fragmentación: Es la capacidad que tiene un AP de dividir la información en tramas más pequeñas.

CAPITULO III

BLUETOOTH

3.1. Qué es Bluetooth?

Figura 9: Aplicaciones de la Tecnología Bluetooth

Bluetooth es una tecnología que provee un camino fácil para la computación móvil, para la comunicación entre dispositivos y conectarse a Internet a altas velocidades, sin el uso de cables. Además, se busca facilitar la sincronización de datos de computadoras móviles, teléfonos celulares y manejadores de dispositivos.

La Tecnología *Bluetooth* es de pequeña escala, bajo costo y se caracteriza por usar enlaces de radio de corto alcance entre móviles y otros dispositivos, como teléfonos celulares, puntos de accesos de red (*access points*) y computadoras. Esta tecnología opera en la banda de 2.4 *GHz*. Tiene la capacidad de atravesar paredes y otros obstáculos, por lo cual es ideal tanto para el trabajo móvil, como el trabajo en oficinas.

3.1.1. Cómo surgió el estándar:

Durante 1994, se comenzó a investigar la posibilidad de crear un dispositivo de bajo costo que sirviera para comunicar diversos dispositivos, la idea era hacerlo basado en un estándar estricto para que su uso se difundiera y diversos fabricantes pudieran desarrollar dispositivos que lo utilizaran. En 1998, un grupo de industrias líderes en computadoras y telecomunicaciones, incluyendo *INTEL, IBM, Toshiba, Ericsson y Nokia*, estuvieron desarrollando dicho dispositivo. Para asegurar, que esta tecnología esta implementada con un empalme perfecto en una amplia gama de dispositivos, esos líderes formaron un grupo de intereses especiales (*Special Interests Group - SIG*). El *SIG* fue rápidamente ganando miembros, como las compañías *3Com, Axis Comunication, Compaq, Dell, Lucent Technologies UK Limited, Motorola, Qualcomm y Xircom.*

3.1.2. Especificaciones de la Tecnología Bluetooth:

La especificación de *Bluetooth* define un canal de comunicación de máximo *720Kbps* con alcance óptimo de 10m (opcionalmente 100m).

La frecuencia de radio con la que trabaja está en el rango de 2.4 a 2.48*GHz* con amplio espectro y saltos de frecuencia con posibilidad de transmitir en *full duplex* con un máximo de 1600 saltos/seg. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1*Mhz*; esto permite brindar seguridad y robustez. La potencia de salida para transmitir a una distancia máxima de 10m es de 0*dBm* (1 *mW*), mientras que la versión de largo alcance transmite entre -30 y 20*dBm* (100 *mW*).

Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se implemento una solución en un solo chip utilizando tecnología de fabricación de circuitos integrados *CMOS*. De esta manera, se logró crear una solución de 9x9mm y que consume aproximadamente 97% menos energía que un teléfono celular común.

El protocolo de banda base (canales simples por línea) combina conmutación de circuitos y paquetes. Para asegurar que los paquetes no lleguen fuera de orden, los *slots* pueden ser reservados por paquetes síncronos, un salto diferente de señal es usado para cada paquete. Por otro lado, el conmutador de circuitos puede ser asíncrono o síncrono.

Tres canales de datos síncronos (voz), o un canal de datos síncrono y uno asíncrono, pueden ser soportados en un solo canal. Cada canal de voz puede soportar una tasa de transferencia de 64 *Kbps* en cada sentido, la cual es suficientemente adecuada para la transmisión de voz. Un canal asíncrono, máximo puede transmitir 721 *Kbps* en una dirección y 56 *Kbps* en la dirección opuesta, sin embargo, para una conexión asíncrona es posible soportar 432,6 *Kbps* en ambas direcciones si el enlace es simétrico.

3.2. Arquitectura de Hardware

El Hardware que compone el dispositivo *Bluetooth* esta compuesto por dos partes. Un dispositivo de radio, en cargado de modular y transmitir la señal; y un controlador digital. El controlador digital esta compuesto por un CPU, por un procesador de señales digitales (*DSP - Digital Signal Processor*) llamado *Link Controller* (o controlador de Enlace) y de los interfaces con el dispositivo anfitrión.

El *LC o Link Controller* está encargado de hacer el procesamiento de la banda base y del manejo de los protocolos *ARQ y FEC* de capa física. Además, se encarga de las funciones de transferencia (tanto asíncrona como síncrona), codificación de audio y encriptación de datos.

La CPU del dispositivo se encarga de atender las instrucciones relacionadas con *Bluetooth* del dispositivo anfitrión, para así simplificar su operación. Para ello, sobre la CPU corre un software denominado Link Manager que tiene la función de comunicarse con otros dispositivos por medio del protocolo *LMP*.

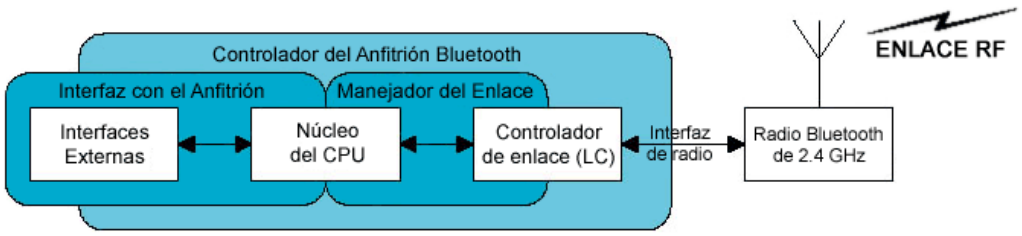


Figura 10: Arquitectura de Hardware de un Bluetooth

Entre las tareas realizadas por el *LC y el Link Manager*, destacan las siguientes:

- Envío y Recepción de Datos.
- Empaginamiento y Peticiones.
- Determinación de Conexiones.
- Autenticación.
- Negociación y determinación de tipos de enlace, por ejemplo *SCO o ACL*
- Determinación del tipo de cuerpo de cada paquete.
- Ubicación del dispositivo en modo *sniff o hold.*

3.3. Arquitectura de Software

Buscando ampliar la compatibilidad de los dispositivos *Bluetooth*, los dispositivos que se apegan al estándar utilizan como interfaz entre el dispositivo anfitrión (*laptop*, teléfono celular, etc) y el dispositivo *Bluetooth* como tal (chip *Bluetooth*) una interfaz denominada *HCI (Host Controller Interface).*

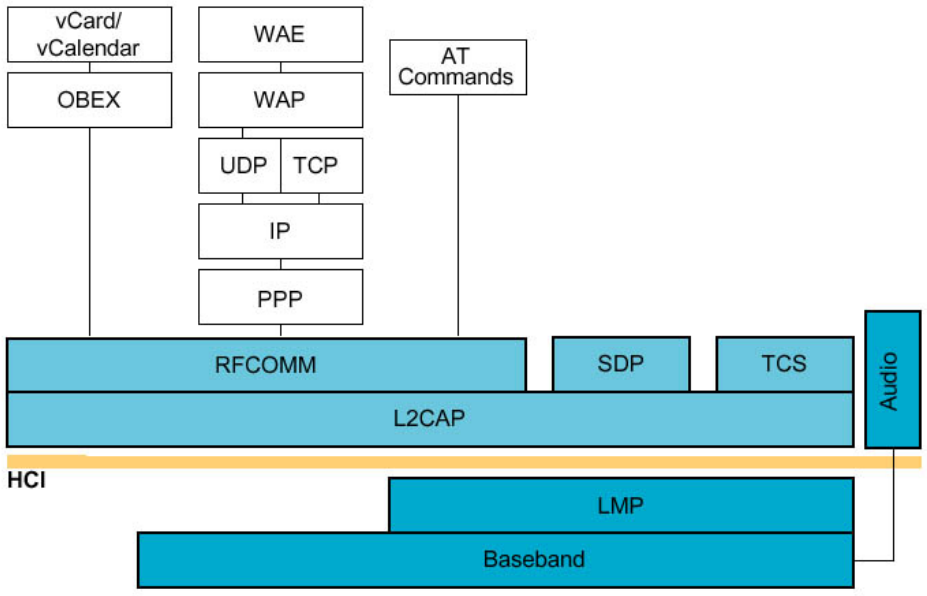


Figura 11: Modelo de Capas y Protocolos de un Bluetooth

Los protocolos de alto nivel como el *SDP* (Protocolo utilizado para encontrar otros dispositivos *Bluetooth* dentro del rango de comunicación, encargado, también, de detectar la función de los dispositivos en rango), *RFCOMM* (Protocolo utilizado para

emular conexiones de puerto serial) y *TCS* (Protocolo de control de telefonía) interactúan con el controlador de banda base a través del Protocolo *L2CAP (Logical Link Control and Adaptation Protocol).* El protocolo *L2CAP* se encarga de la segmentación y reensamblaje de los paquetes para poder enviar paquetes de mayor tamaño a través de la conexión *Bluetooth*.

La pila completa se compone tanto de protocolos específicos de *Bluetooth* (LM (Link Manager) y *L2CAP (Logical Link Control Adaption Protocol),* por ejemplo) como de protocolos no específicos de *Bluetooth* como son *OBEX (Objects Exchange Protocol), UDP (User Datagram Protocol), TCP, IP,* etc. Debido a que la hora de diseñar la torre de protocolos, el objetivo principal ha sido maximizar el número de protocolos existentes que se puedan reutilizar en las capas más altas para diferentes propósitos.

A parte de todos estos protocolos, la especificación define el *HCI (Host Controller Interface),* que se encarga de proporcionar una interfaz de comandos al controlador *BaseBand,* al gestor de enlace, y nos da acceso al estado del *Hardware* y a los registros de control.

3.3.1. Descripción de los protocolos:

3.3.1.1. Link Manager (LM) y Link Manager Protocol (LMP).

El *Link Manager* es el sistema que consigue establecer la conexión entre dispositivos. Se encarga del establecimiento, la autentificación y la configuración del enlace.

El Link Manager localiza a otros gestores y se comunica con ellos gracias al protocolo de gestión del enlace *LMP*.

Para poder realizar su función de proveedor de servicio, el *LM* utiliza los servicios incluidos en el controlador de enlace (LC, "*Link Controller*").

El *Link Manager Protocol* básicamente consiste en un número de *PDUs (Protocol Data Units)* que son enviadas de un dispositivo a otro.

A continuación se enuncian los servicios soportados:

- Transmisión y recepción de datos.
- Petición de nombre: El gestor de enlace tiene un eficiente método para inquirir y reportar la *ID* de un dispositivo con una longitud de máximo 16 caracteres.
- Petición de las direcciones de enlace.
- Establecimiento de la conexión.
- Autentificación.
- Negociación del modo de enlace y establecimiento, por ejemplo, modo datos o modo voz/datos. Esto puede cambiarse durante la conexión.

3.3.1.1.1. Modos.

Establecimiento de un dispositivo al modo "*sniff*". En este modo se reduce el ciclo de trabajo de una estación esclava, ya que sólo escucha cada M *slots*, siendo el valor de M negociado con el gestor de enlace. La estación maestra puede sólo comenzar la transmisión en tiempos/*slots* específicos, separados estos por intervalos regulares.

Mantenimiento de un dispositivo de enlace en espera. En modo espera, el apagado del receptor durante períodos de tiempo más largos ahorra energía. Cualquier entidad puede volver a establecer un enlace, con una latencia media de 4 segundos. Esto es definido por el gestor de enlace y manejado por el controlador de enlace.

Establecimiento de un dispositivo en modo "aparcado": Esto es útil cuando un dispositivo no necesita participar activamente en el canal, pero sí quiere permanecer sincronizado. En este modo dicha entidad "despierta" en intervalos regulares de tiempo para escuchar al canal y así poder re-sincronizarse con el resto de entidades de la *piconet.*

3.3.1.2. Interfaz de la Controladora de la Máquina (*HCI*).

La interfaz de la Controladora de la Máquina (*Host Controller Interface*) proporciona una interfaz de comandos para la controladora de banda base y para el gestor de enlace, y permite acceder al estado del *Hardware* y a los registros de control. Esta interfaz

proporciona una capa de acceso homogénea para todos los dispositivos *Bluetooth* de banda base.

La capa *HCI* de la máquina intercambia comandos y datos con el *firmware del HCI* presente en el dispositivo *Bluetooth*. El *driver* de la capa de transporte de la controladora de la máquina (es decir, el *driver* del bus físico) proporciona ambas capas de *HCI* la posibilidad de intercambiar información entre ellas.

Una de las tareas más importantes de *HCI* que se deben realizar, es el descubrimiento automático de otros dispositivos *Bluetooth* que se encuentren dentro del radio de cobertura. Esta operación se denomina en inglés *inquiry* (consulta). Hay que tener presente que un dispositivo remoto sólo contesta a la consulta si se encuentra configurado en modo visible (*discoverable mode*).

BD_ADDR: Es la dirección identificativa única del dispositivo *Bluetooth,* similar a las direcciones *MAC* de las tarjetas *Ethernet*. Esta dirección se necesita para transmitir otro tipo de información a otros dispositivos.

Si se realiza una consulta (*inquiry*) sobre el dispositivo *Bluetooth* remoto, dicho dispositivo identificará nuestro computador como "nombre de su sistema (*ubt0*)". El nombre asignado al dispositivo local se puede modificar en cualquier momento.

El sistema *Bluetooth* proporciona una conexión punto a punto (con sólo dos unidades *Bluetooth* involucradas) o también una conexión punto multipunto. En el último caso, la conexión se comparte entre varios dispositivos *Bluetooth*.

3.3.1.3. Protocolo de Adaptación y de Control de Enlace a nivel Lógico (*L2CAP*).

El protocolo *L2CAP (Logical Link Control and Adaptation Protocol)* proporciona servicios de datos tanto orientados a conexión como no orientados a conexión a los protocolos de las capas superiores, junto con facilidades de multiplexación y de segmentación y reensamblaje.

L2CAP permite que los protocolos de capas superiores puedan transmitir y recibir paquetes de datos *L2CAP* de hasta 64 *kBits* de longitud.

L2CAP se basa en el concepto de canales. Un canal es una conexión lógica que se sitúa sobre la conexión de banda base. Cada canal se asocia a un único protocolo. Cada paquete *L2CAP* que se recibe a un canal se redirige al protocolo superior correspondiente. Varios canales pueden operar sobre la misma conexión de banda base, pero un canal no puede tener asociados más de un protocolo de alto nivel.

Una herramienta de diagnóstico interesante es *btsockstat, para FreeBSD*. Realiza un trabajo similar al comando netstat, pero en este caso para las estructuras de datos relacionadas con el sistema *Bluetooth.*

3.3.1.4. Protocolo *RFCOMM*.

El protocolo *RFCOMM* proporciona emulación de puertos serie a través del protocolo *L2CAP*. Este protocolo se basa en el estándar de la *ETSI* denominado TS 07.10. *RFCOMM* es un protocolo de transporte sencillo, con soporte para hasta 9 puertos serie *RS-232 (EIATIA-232-E).* El protocolo *RFCOMM* permite hasta 60 conexiones simultáneas (canales *RFCOMM*) entre dos dispositivos *Bluetooth*.

Para los propósitos de *RFCOMM*, un camino de comunicación involucra siempre a dos aplicaciones que se ejecutan en dos dispositivos distintos (los extremos de la comunicación). Entre ellos existe un segmento que los comunica. *RFCOMM* pretende cubrir aquellas aplicaciones que utilizan los puertos serie de las máquinas donde se ejecutan. El segmento de comunicación es un enlace *Bluetooth* desde un dispositivo al otro (conexión directa).

RFCOMM trata únicamente con la conexión de dispositivos directamente, y también con conexiones entre el dispositivo y el modem para realizar conexiones de red. *RFCOMM* puede soportar otras configuraciones, tales como módulos que se comunican vía *Bluetooth* por un lado y que proporcionan una interfaz de red cableada por el otro.

3.3.1.5. Protocolo de Descubrimiento de Servicios (*SDP*).

El Protocolo de Descubrimiento de Servicios (*Service Discovery Protocol o SDP*) permite a las aplicaciones cliente descubrir la existencia de diversos servicios

proporcionados por uno o varios servidores de aplicaciones, junto con los atributos y propiedades de los servicios que se ofrecen.

Estos atributos de servicio incluyen el tipo o clase de servicio ofrecido y el mecanismo o la información necesaria para utilizar dichos servicios.

SDP se basa en una determinada comunicación entre un servidor *SDP* y un cliente *SDP*.

El servidor mantiene una lista de registros de servicios, los cuales describen las características de los servicios ofrecidos. Cada registro contiene información sobre un determinado servicio. Un cliente puede recuperar la información de un registro de servicio almacenado en un servidor *SDP* lanzando una petición *SDP*. Si el cliente o la aplicación asociada con el cliente deciden utilizar un determinado servicio, debe establecer una conexión independiente con el servicio en cuestión. *SDP* proporciona un mecanismo para el descubrimiento de servicios y sus atributos asociados, pero no proporciona ningún mecanismo ni protocolo para utilizar dichos servicios.

Normalmente, un cliente *SDP* realiza una búsqueda de servicios acotada por determinadas características. No obstante hay momentos en los que resulta deseable descubrir todos los servicios ofrecidos por un servidor *SDP* sin que pueda existir ningún conocimiento previo sobre los registros que pueda contener. Este proceso de búsqueda de cualquier servicio ofrecido se denomina navegación o *browsing*.

Resulta importante resaltar una vez más que cada servicio posee una lista de atributos (por ejemplo en el canal *RFCOMM*). Dependiendo de los servicios que se quieran utilizar puede resultar necesario anotar algunos de los atributos. Algunas implementaciones de *Bluetooth* no soportan navegación de servicios y pueden devolver una lista vacía.

3.4. La Seguridad en Bluetooth

3.4.1. Modos de seguridad.

Hay tres modos primarios de seguridad.

- Modo 1. Sin seguridad. Todos los mecanismos de seguridad (autenticación y cifrado) están deshabilitados. Además el dispositivo se sitúa en modo promiscuo, permitiendo que todos los dispositivos *Bluetooth* se conecten a él.
- Modo 2. En la capa *L2CAP*, nivel de servicios. Los procedimientos de seguridad son inicializados después de establecerse un canal entre el nivel *LM* y el de *L2CAP*. Un gestor de seguridad controla el acceso a servicios y dispositivos. Variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos de seguridad que operen en paralelo. Su interfase es muy simple y no hay ninguna codificación adicional de *PIN* o claves.
- Modo 3. En el nivel de *Link*. Todas las rutinas están dentro del chip *Bluetooth* y nada es transmitido en plano. Los procedimientos de seguridad son iniciados antes de establecer algún canal. Aparte del cifrado tiene autenticación *PIN* y seguridad *MAC*. Su metodología consiste en compartir una clave secreta de enlace (clave de *linkado*) entre un par de dispositivos. Para generar esta clave, se usa un procedimiento de "*pairing*" cuando los dos dispositivos se comunican por primera vez.

3.4.2. Emparejamiento de Dispositivos.

Por defecto, la comunicación *Bluetooth* no se valida, por lo que cualquier dispositivo puede en principio hablar con cualquier otro. Un dispositivo *Bluetooth* (por ejemplo un teléfono celular) puede solicitar autenticación para realizar un determinado servicio (por ejemplo para el servicio de marcación por modem).

La autenticación de *Bluetooth* normalmente se realiza utilizando códigos *PIN*. Un código *PIN* es una cadena *ASCII* de hasta 16 caracteres de longitud. Los usuarios deben introducir el mismo código *PIN* en ambos dispositivos.

Una vez que el usuario ha introducido el *PIN* adecuado ambos dispositivos generan una clave de enlace. Una vez generada, la clave se puede almacenar en el propio dispositivo o en un dispositivo de almacenamiento externo. La siguiente vez que se comuniquen ambos dispositivos se reutilizará la misma clave.

El procedimiento descrito hasta este punto se denomina emparejamiento (*pairing*). Es importante recordar que si la clave de enlace se pierde en alguno de los dispositivos involucrados se debe volver a ejecutar el procedimiento de emparejamiento.

No existe ninguna limitación en los códigos *PIN* a excepción de su longitud. Algunos dispositivos (por ejemplo los dispositivos de mano *Bluetooth*) pueden obligar a escribir un número predeterminado de caracteres para el código *PIN*.

3.4.3. Inicialización y Generación de la claves.

La Clave de *Linkado* es generada durante una fase de inicialización, cuando dos dispositivos empiezan a comunicarse. Según la especificación *Bluetooth*, la clave es generada durante la fase de inicialización cuando el usuario introduce un *PIN* idéntico en ambos dispositivos. Después de completarse la inicialización, los dispositivos se autentican de manera automática y transparente y se lleva a cabo el cifrado de la conexión.

3.4.4. Autenticación Bluetooth

El procedimiento de autenticación sigue el conocido esquema "*challenge-response*" (desafío-respuesta).

3.4.5. Generación de la clave de cifrado.

Cuando el Link Manager (*LM)* activa el cifrado, se crea la Clave de Cifrado (*Kc*), que es modificada cada vez que el dispositivo entra en dicho modo.

3.4.6. Proceso de cifrado en Bluetooth.

La especificación de *Bluetooth*, como vemos permite tres modos de cifrado diferentes.

- Modo 1. Ninguna parte del tráfico de datos es cifrada.
- Modo 2. El tráfico general va sin cifrar, pero el tráfico dirigido individualmente se cifra según las claves individuales de la conexión.
- Modo 3. Todo el tráfico es cifrado acorde a la Clave de Cifrado.

La información de usuario es protegida por cifrado de la carga útil (*payload*), ya que el código de acceso y la cabecera del paquete nunca son cifrados. Consiste básicamente de tres partes.

- Una parte que realiza la inicialización (generación de la clave de carga útil).
- Una segunda parte que es el generador de cadenas de claves
- Una tercera parte en la cual se realiza el cifrado o el descifrado.

El Generador de Clave de *KeyStream* combina los *bits* de entrada de una forma apropiada y los guarda en 4 registros de desplazamiento retroalimentados, conocidos como *Linear Feedback Shift Registers* (*LSFR*). Estos registros son de 25, 31, 33 y 39 bits (128 en total). Este método viene derivado del generador de cifrado de *Streams de Massey y Rueppel*.

Cuando el cifrado está activo, el maestro envía un número aleatorio (*RAND*) al esclavo. Antes de la transmisión de cada paquete, el *LFSR* se inicializa en el Generador de Clave de Carga mediante la combinación de *RAND*, la identificación del maestro, la clave de cifrado *Kc* y el número de reloj (o número de *Slot*).

Como el tamaño de la Clave de Cifrado varía desde 8 a 128 *bits*, tiene que ser "negociado" entre los dispositivos previamente. En cada dispositivo hay un parámetro que define la longitud máxima permitida de la clave. En esta negociación, el maestro manda su sugerencia al esclavo, y este puede aceptarla o enviar otra sugerencia. Así hasta que haya consenso entre los dispositivos, o uno de ellos aborte la negociación. En cada aplicación, hay definido un tamaño mínimo de clave aceptable, y si estos

requerimientos no son cumplidos por ambos dispositivos, la aplicación aborta la negociación, y el cifrado no puede ser usado. Esto es necesario para evitar la situación donde uno de los dispositivos fuerce un cifrado débil algún fin malicioso.

Finalmente se genera el *KeyStream (K cipher)*. El descifrado se realizará exactamente de la misma manera usando la misma clave que se usó para el cifrado.

Cada paquete de carga útil es cifrado separadamente, lo cual se consigue si tenemos en cuenta que se utiliza el reloj del maestro, el cual cambia una unidad cada intervalo de tiempo (*625μs*), por lo que la clave de carga útil será diferente para cada paquete, excepto para aquellos que ocupen más de un intervalo de tiempo, en cuyo caso el valor del reloj del primer intervalo de tiempo del paquete será el que se utilizará para todo el paquete.

3.4.7. Debilidades de la seguridad en Bluetooth.

Generales

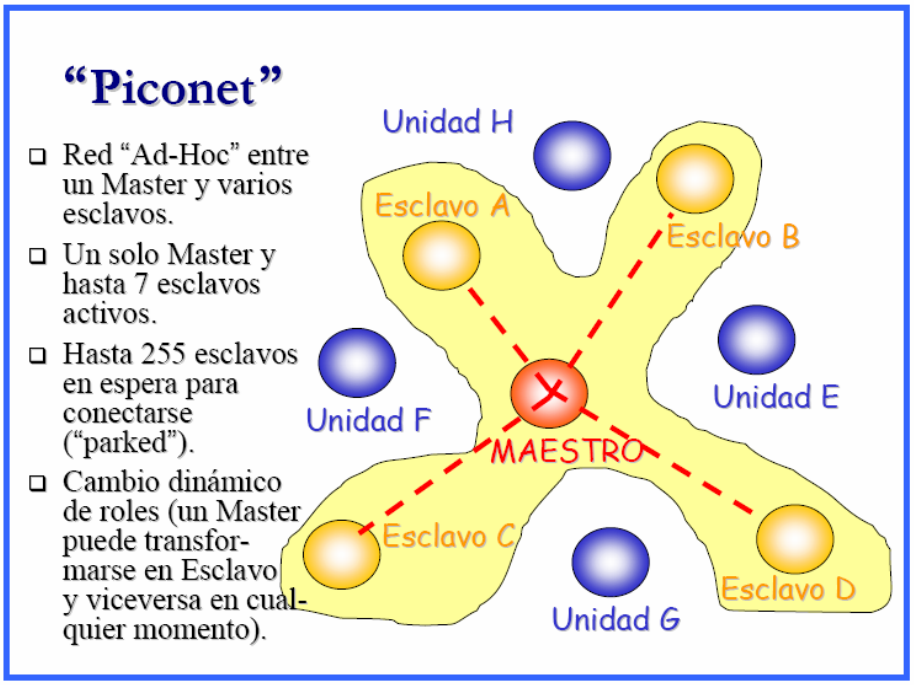
- No está demostrada la fuerza del generador pseudo aleatorio del procedimiento "*Challenge-Response*". Se podrían producir números estáticos o repeticiones periódicas que redujeran su efectividad.
- *PIN*s cortos son permitidos. De hecho se puede elegir la longitud del *PIN*, que va de entre 1 a 16 *Bytes*. Normalmente los usuarios los prefieren muy cortos.
- No hay una forma "elegante" de generar y distribuir el *PIN*. Establecer *PIN*s en una red *Bluetooth* grande y con muchos usuarios puede ser difícil, y esto lleva normalmente a problemas de seguridad.
- La longitud de la clave de cifrado es negociable. Es necesario un procedimiento de generación de claves más fuerte.
- En el caso del modo 3, la clave maestra es compartida. Es necesario desarrollar un esquema de transmisión de claves mejorado.
- No existe autenticación de usuarios. Sólo está implementada la autenticación de dispositivos.
- No hay límite de intentos de autenticación.
- El algoritmo de cifrado es muy débil.

- La autenticación es un simple "*challenge-response*" con *hashes*. Según esta diseñado, el esquema es vulnerable a ataques "*Man in the Middle*".
- Los servicios de seguridad son limitados. Servicios de auditoria, de no repudio, etc., no están implementados.

3.5. Topología de Redes *Bluetooth*

La topología de las redes *Bluetooth* puede ser:

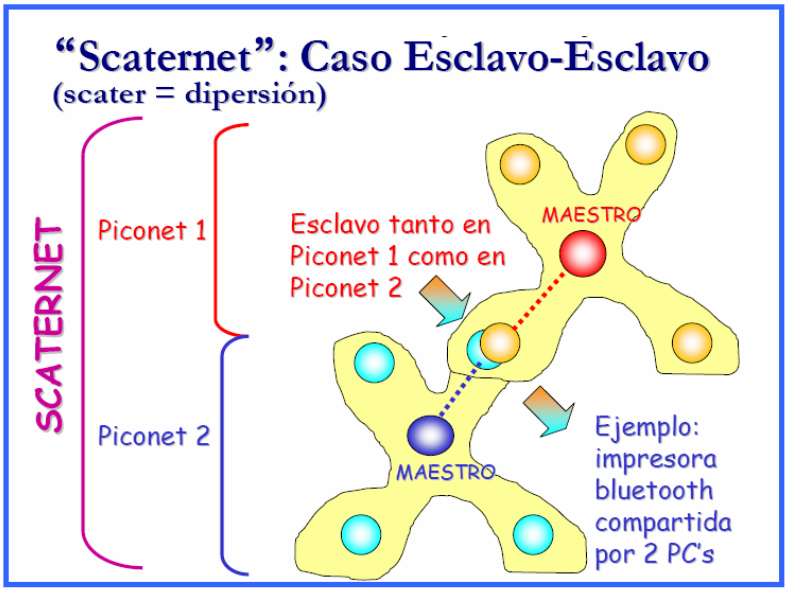
Piconet:



[6]Figura 12: Topología Piconet

[6] Ing. Martín Vernengo, mvernel@fi.uba.ar Curso Argentina Wlan

Scaternet:



[7]Figura 13: Topología Scaternet

Los dispositivos, se comunican en redes denominadas *piconets*. Estas redes tienen posibilidad de crecer hasta tener 8 conexiones punto a punto. Además, se puede extender la red mediante la formación de *scatternets*. Una *scatternet* es la red producida cuando dos dispositivos pertenecientes a dos *piconets* diferentes, se conectan.

En una *piconet*, un dispositivo debe actuar como *master*, enviando la información del reloj (para sincronizarse) y la información de los saltos de frecuencia. El resto de los dispositivos actúan como *slaves*.

3.5.1. Transmisión

Bluetooth esta diseñado para usar acuses de recibos (*acknowledgement*) y saltos de frecuencias (*frecuency hopping*), lo cual hará conexiones robustas. Esto esta basado en paquetes, y saltarán a una nueva frecuencia después de que cada paquete es recibido, lo cual no solo ayuda a los problemas de interferencia, sino que añade seguridad. La tasa de transmisión de datos es un *Mbps*, incluyendo el encabezado. Una transmisión "*full duplex*" (ambas direcciones al mismo tiempo) es realizado por *multiplexaje* de división de tiempo.

[7] Ing. Martín Vernengo, mvernel@fi.uba.ar Curso Argentina Wlan

Como se especificó previamente, la transmisión de datos puede ser realizada de maneta síncrona o asíncrona. El método Síncrono Orientado a Conexión (SCO) es usado principalmente para voz, y el Asíncrono No Orientado a Conexión (*ACL*) es principalmente usado para transmitir datos. Dentro de un "*piconet*" cada par *master-slave* pueden usar un modo de transmisión distinto, y los modos pueden ser cambiados en algún momento. La división de tiempo "*Duplex*", es usado para *SCO y ACL*, y ambos soportan 16 tipos de paquetes, cuatro de los cuales son paquetes de control, que son los mismos en cada tipo . Debido a la necesidad de tranquilidad en la transmisión de datos, los paquetes *SCO* son entregados en intervalos reservados, esto es, los paquetes son enviados en grupos sin permitir la interrupción de otras transmisiones. Los enlaces *ACL* soportan tanto transmisión simétrica como transmisión asimétrica.

3.5.2. Protocolo de Conexión

Las conexiones *Bluetooth*, son establecidas a través de la siguiente técnica:

- *Standby*: Los dispositivos en un "piconet" que no están conectados, están en modo standby, ellos escuchan mensajes cada 1,28 segundos, sobre 32 saltos de frecuencias.
- *Page/Inquiry*: Si un dispositivo desea hacer una conexión con otro dispositivo, éste le envía un mensaje de tipo page, si la dirección es conocida; o una petición a través de un mensaje de *page*, si éste no es conocido. La unidad "*master*" envía 16 *page message* idénticos, en 16 saltos de frecuencias, a la unidad "*slave*". Si no hay respuesta, el "*master*" retransmite en los otros 16 saltos de frecuencia. El método de Petición (*inquiry*) requiere una respuesta extra por parte de la unidad "*slave*", desde la dirección *MAC*, que no es conocida por la unidad "*master*".
- *Active:* Ocurre la transmisión de datos.
- *Hold:* Modo en el que no se requiere transmisión de datos entre el "*master*" o el "*slave*". El objetivo de esto es conservar el poder.
- *Sniff:* El modo *sniff*, es aplicable solo para las unidades "*slaves*", es para conservar el poder. Durante este modo, el "*slave*", no toma un rol activo en la "*piconet*", pero escucha a un reducido nivel.

- *Park:* El modo park es un nivel más reducido, que el modo *hold*. Durante este, el "*slave*" es sincronizado a la "*piconet*", por eso no requiere un reactivación completa, pero no es parte del tráfico. En este estado, ellos no tienen direcciones *MAC* y solo escuchan para mantener su sincronización con el "*master*" y chequear los mensajes de *broadcast*.

3.5.3. Seguridad y Corrección de Errores

Se definen tres técnicas de corrección de error:

- *1/3 rate forward error correction code (FEC),* este método es diseñado para reducir el número de retransmisiones.
- *2/3 rate forward error correction code FEC.*
- *Automatic Repeat Request (ARQ).*
- En cuanto a la Seguridad, ésta es provista en tres caminos:
    - A través de saltos de frecuencia pseudos-aleatorios que dificultan que dispositivos ajenos a la red puedan interceptar o ver el tráfico de información.
    - Autentificación, permite a un usuario controlar la conectividad para solo dispositivos especificados.
    - Encriptación, se usan claves secretas con longitudes de 1, 40 o 64 *bits*.

3.6. Modelos de Uso

Algunas de las aplicaciones que se pueden dar a los dispositivos *Bluetooth*, son las siguientes:

- El Teléfono 3 en 1: Se ofrece la posibilidad de utilizar un mismo teléfono sin importar donde se encuentra.
    - Puede funcionar como el teléfono en su casa, si el dispositivo está en el rango de las bases *Bluetooth* ubicadas en su casa.
    - Como teléfono celular-portátil si no se encuentra cerca de las bases de su casa.

  - Como medio de acceso a sus contactos, números de teléfono, *email*, etc.

- Conexión a Internet: El dispositivo *Bluetooth* puede conectarse con cualquier medio que esté conectado a Internet y que a la vez, posea una interfaz *Bluetooth*, para así mantenerlo siempre conectado, ya sea a través de su celular, de su conexión *dial-up* o a través de una red cableada a Internet.
- Dispositivo Manos libres: El uso de este dispositivo permite acceder la información de los contactos, enviar correo electrónico y realizar llamadas sin ocupar las manos. Esta funcionalidad está controlada por voz.
- Laptop como teléfono: Se tiene la posibilidad de utilizar el laptop para realizar llamadas de voz tal cuál se haría con un teléfono.
- Sincronización automática: Constantemente, todos sus dispositivos *Bluetooth* mantienen sincronizada la información, de manera que si modifica alguna información en su *laptop*, y la misma estaba también almacenada en su *PDA* o en su celular, el cambio se refleje allí también.
- Escritorio Inalámbrico: *Bluetooth* ofrece la posibilidad de eliminar todos los cables (excepto los de poder) que suelen invadir los escritorios, tanto en los hogares como en las oficinas.

3.7. Problemas y Desventajas

Como todo, la tecnología *Bluetooth*, también presenta algunos problemas que solucionar. Los *microchips* no son baratos aún, se espera que dentro de unos años disminuyan los costos, de lo contrario, el objetivo de esta tecnología no sería alcanzado. Por su parte, la velocidad de transmisión, aunque considerable, pronto quedará disminuida, debido a la capacidad de los móviles de tercera generación. Y a pesar de que los prototipos de dispositivos *Bluetooth* se reproducen rápidamente, no sucede lo mismo con los programas informáticos que deben regular su funcionamiento.

Además, el espectro de radiofrecuencia en el que opera no está regulado para el uso público en todos los países. En lugares como Francia o España el uso del espectro está restringido y se requiere la aprobación explícita del gobierno para poder operar en la banda *ISM*.

Con miles de compañías diseñando productos y aplicaciones *Bluetooth,* será difícil mantenerlas a todas bajo el mismo manto.

Aun así, las desventajas son mínimas cuando se comparan con los beneficios de disfrutar de un mundo sin cables y con las flexibilidades que ofrecería un mundo interconectado de manera inalámbrica y sin altos costos de conexión.

CAPITULO IV

INSTALACION DE DISPOSITIVOS

4.1 Instalación de Hardware.

4.1.1 Wi-Fi

Los últimos modelos de Pcs portátiles traen incorporado la tecnología de conexiones inalámbricas como *Wi-Fi*, sin embargo para lograr nuestra aplicación práctica utilizaremos un dispositivo Wireless externo indicado en la figura 14

Figura 14: Tarjeta Wireless 32 bits

Procedemos a insertar la tarjeta en la ranura de expansión de 32 bits, luego realizamos la instalación del respectivo controlador, que el fabricante nos proporciona, y software adicional si este posee.

Figura 15: Autorun de disco Instalación

4.1.2. Bluetooth

Para la práctica también necesitaremos la instalación del hardware, Wireless USB Bluetooth Adapter.

Figura 16: Dispositivo USB Bluetooth

Este dispositivo será colocado en el puerto *USB* y posteriormente instalado el correspondiente controlador que nos permitirá su configuración.

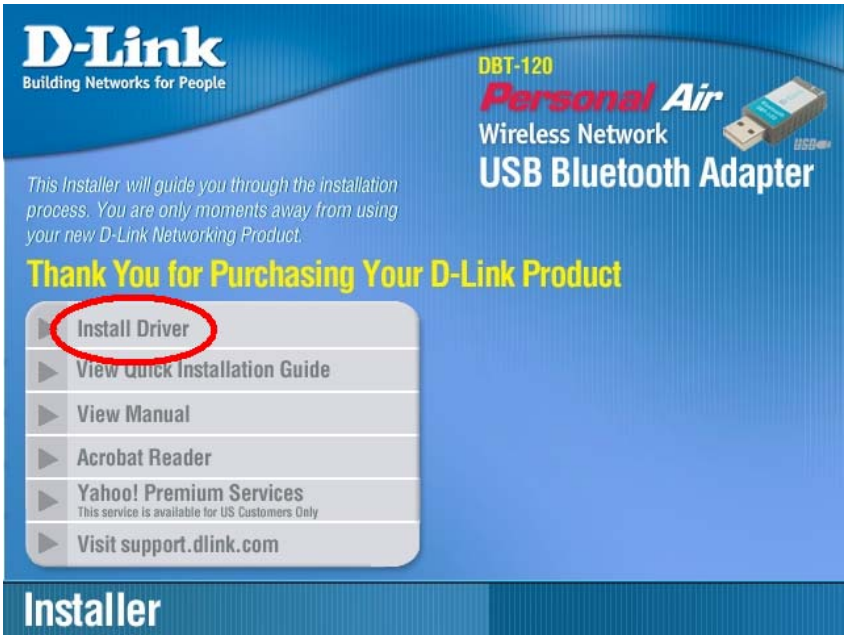


Figura 17: Autorun de disco Instalación

4.2. Configuración De La Red Punto A Punto.

4.2.1. Wi-Fi

Procedemos a la configuración de las tarjetas de red *Wi-Fi* para lograr la interconexión entre los dos equipos. Para esto nos dirigimos al panel de control y seleccionamos el icono *conexiones de red*. Clic en el icono de Conexión de Redes Inalámbricas:

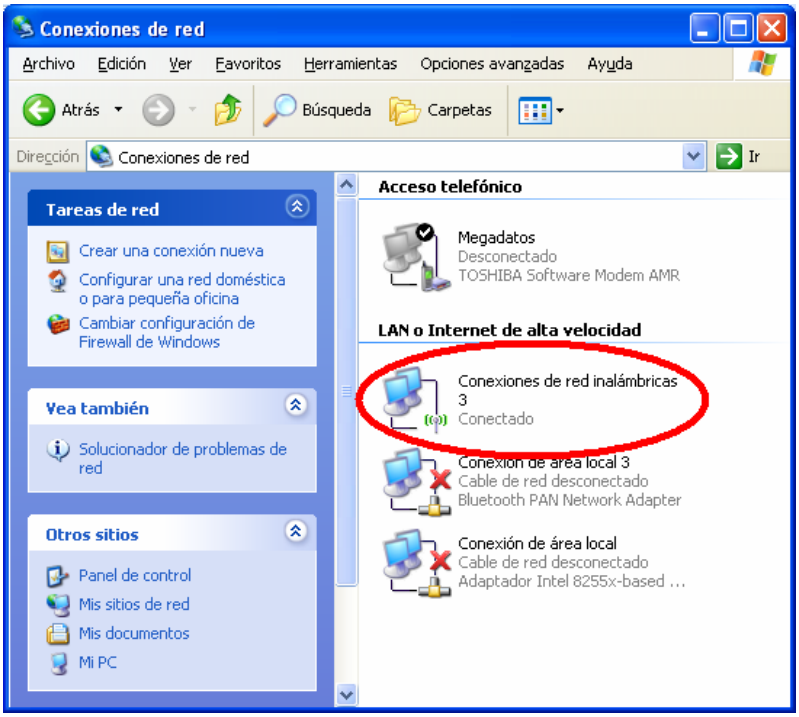


Figura 18: Pantalla de Conexiones de red

Luego seleccionamos la opción *propiedades*:

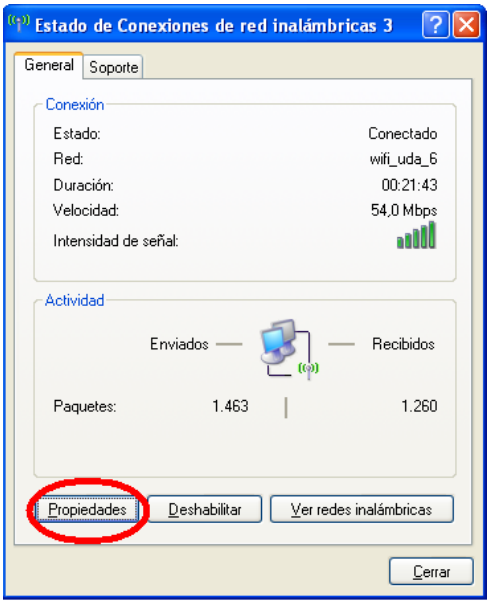


Figura 19: Pantalla de Estado de Conexiones de red

Posteriormente elegimos la opción *protocolo Internet (TCP/IP)* y damos clic en *propiedades*:

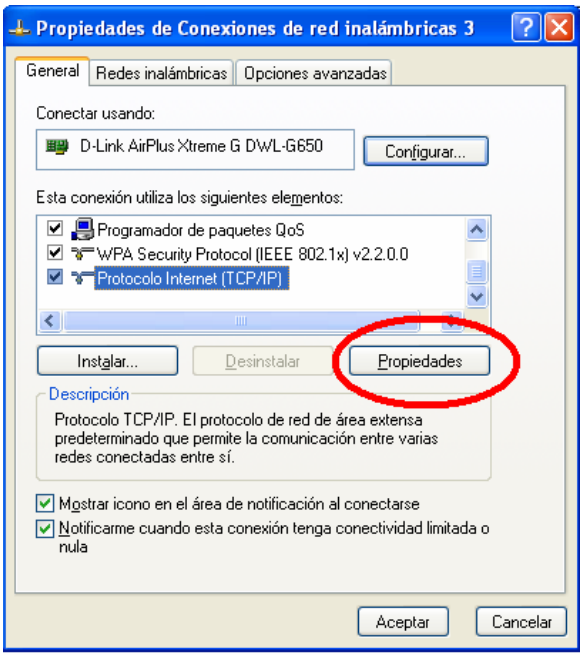


Figura 20: Ventana de Propiedades de Conexiones de red

Entonces, se procede a colocar una dirección IP valida con su respectiva máscara, para poder realizar la configuración, en este caso utilizaremos la dirección 192.168.47.10/ 255.255.255.0 para el primer equipo y 192.168.47.20/255.255.255.0 para el otro equipo.

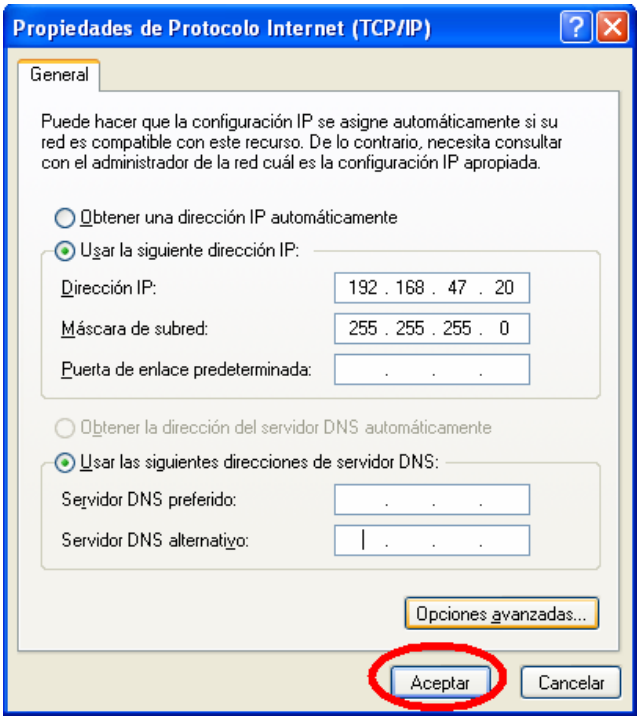


Figura 21: Ventana de Propiedades del Protocolo Internet

Finalmente para establecer la conexión entre los dos equipos, se da clic derecho en la barra de tareas en el icono de *conexiones inalámbricas*, escogemos la opción *ver redes inalámbricas disponibles*.

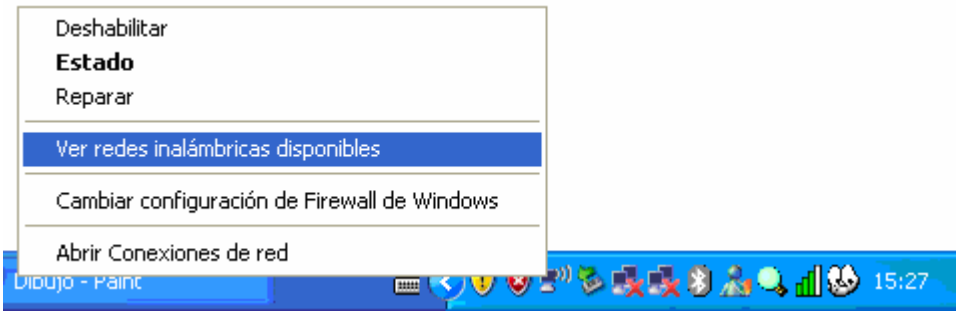


Figura 22: Configuración de Red

A continuación se selecciona la red link *ad-hoc* y luego *conectar*.

4.2.2 Bluetooth

Para lograr la interconexión entre los dos equipos, se procede a la configuración del servicio de Acceso LAN de Bluetooth. Para esto nos dirigimos al *panel de control* y seleccionamos *conexiones de red.* Doble clic en el icono *Bluetooth*:

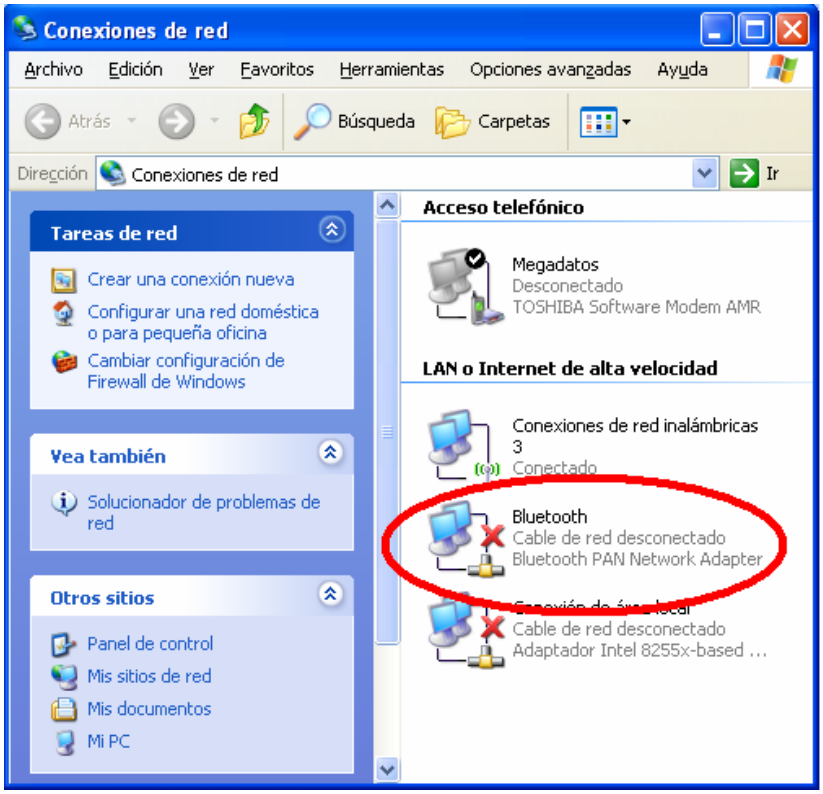


Figura 23: Ventana de Conexiones de red de Bluetooth

Después elegimos la opción *protocolo Internet (TCP/IP)* y damos clic en *propiedades*:

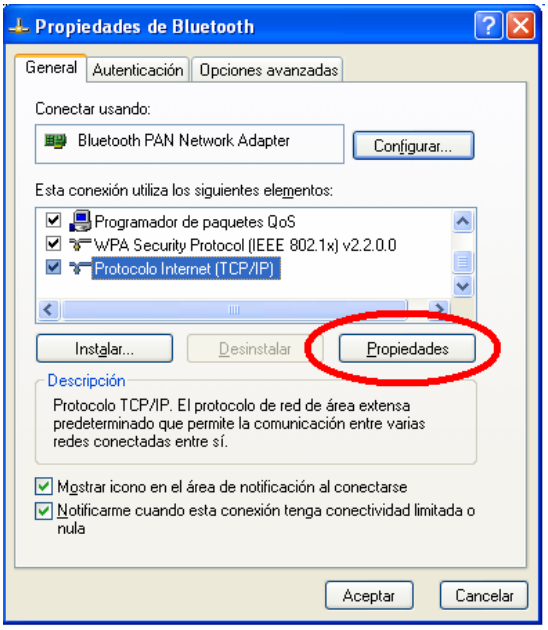


Figura 24: Pantalla de Propiedades de Bluetooth

A continuación se procede a colocar una dirección de red válida con su respectiva máscara, para poder realizar la conexión, en este caso utilizaremos la dirección 192.168.47.30/ 255.255.255.0 para uno de los equipos y la 192.168.47.40/255.255.255.0 para el otro.

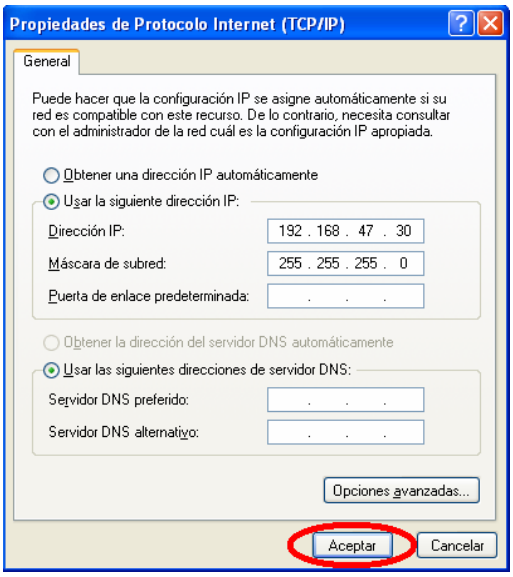


Figura 25: Pantalla de Propiedades de Protocolo Internet

Finalmente para establecer la conexión entre los dos equipos procederemos a dar clic con el botón derecho en la barra de tareas en el icono de *Bluetooth*, seleccionamos la opción *visualizar*.

Figura 26: Conexión de Bluetooth

A continuación nos muestra el asistente para la configuración de los servicios que ofrece *Bluetooth*, para nuestro caso escogemos la opción: *Buscar un dispositivo Bluetooth y configurar como el equipo utilizara sus servicios*.

Figura 27: Consola de Bluetooth

Con lo que procederá a buscar los dispositivos *Bluetooth* cercanos con los que nos podemos conectar. Seleccionamos el dispositivo con el cual necesitamos establecer la conexión y clic en *siguiente*.

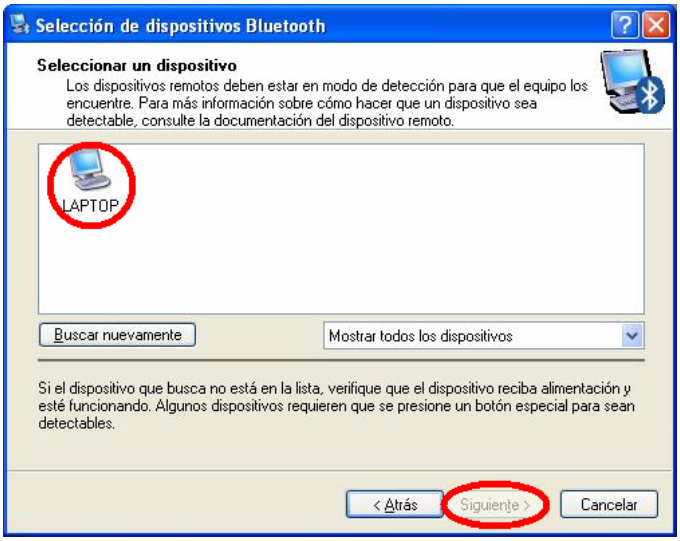


Figura 28: Selección de Dispositivos Bluetooth

Después procederemos a introducir una clave *PIN* y clic en *Iniciar emparejamiento*.

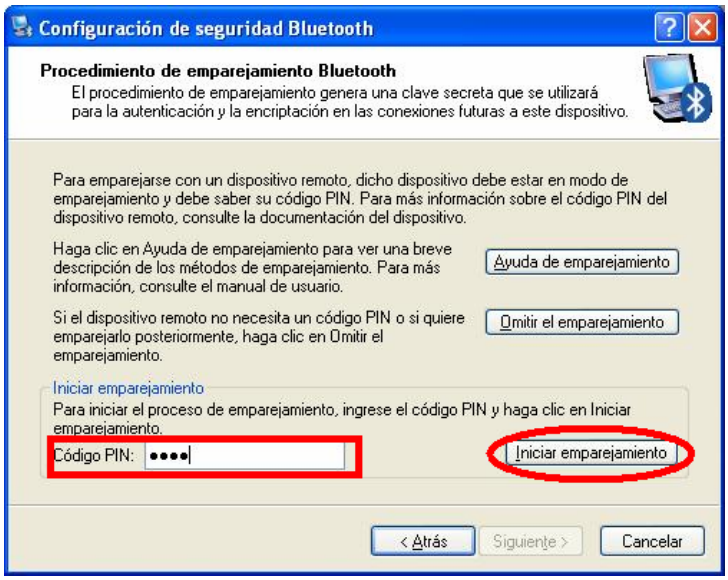


Figura 29: Configuración de seguridad Bluetooth

En esta pantalla (figura 30) se escogerá el tipo de servicio que vamos a utilizar para nuestro caso una red *Ad-hoc*. Clic en finalizar.

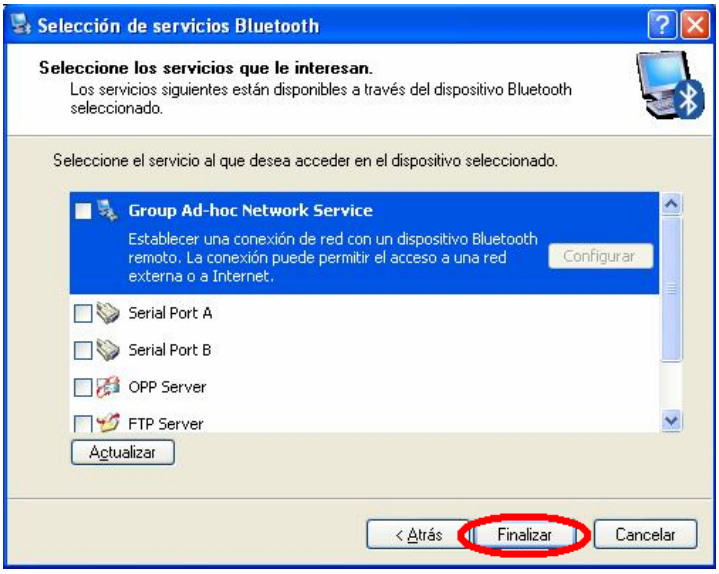


Figura 30: Selección de servicios Bluetooth

Por ultimo en el dispositivo *Bluetooth* remoto nos pedirá el *PIN* que se introdujo en la configuración de quien pidió la conexión.

Figura 31: Introduzca la Contraseña de Bluetooth

Con estos pasos queda establecida la conexión entre los dos dispositivos *Bluetooth.*

CAPITULO V

PRUEBAS DE TRANSMISION DE DATOS

La transmisión de los datos en cuanto a tiempo, depende en gran parte de los dispositivos que se estén utilizando, para nuestra aplicación en lo que se refiere a *Bluetooth* se utilizó un dispositivo que se conecta a 1*Mbs* y otro que se conecta a 10*Mbs*.

En lo que se refiere a *Wi-Fi* uno que se conecta a 108*Mbs* y otro que se conecta 11*Mbs*.

Cabe indicar que las pruebas se realizaron con una conexión punto a punto.

5.1. Operación a diferentes distancias

5.1.1. Bluetooth.

En la prueba realizada se observo que estos dispositivos no tienen un buen desempeño a grandes distancias ya que al alcanzar más de los 10 metros de distancia entre equipos se pierde la conexión.

5.1.2. Wi-Fi

En cuanto a *Wi-Fi* las pruebas realizadas nos indicaron que esta tecnología en la actualidad soporta mayores distancias que *Bluetooth* y que esta en función de la intensidad de señal para lograra mayor eficiencia en la conexión establecida. La distancia máxima que estos dispositivos pueden alcanzar para mantener una conexión puede llegar a 100 metros.

5.2. Desempeño a diferentes tamaños de paquetes de información

5.2.1. Bluetooth y Wi-Fi

La prueba con tamaños de información de 5, 10, 20 *Mbps*, indico, que sin importar la cantidad de información que se transmita, dependerá de la velocidad a la que se conectaron los dispositivos.

5.3. Desempeño a diferentes ambientes.

5.3.1. Bluetooth

El funcionamiento óptimo de esta tecnología se da siempre y cuando los equipos conectados se encuentren en el mismo ambiente, en las pruebas realizadas se detectó que al ser ubicados en diferentes ambientes así la distancia sea cercana la conexión es inestable o nula.

5.3.2. Wi-Fi

El funcionamiento de *Wi-Fi* en diferentes ambientes, es mucho más eficiente, y soporta la conexión en habitaciones y pisos separados, a mayor distancia del *AP* menor la intensidad de la señal.

CONCLUSIONES

Luego de haber realizado el estudio de cada una de las tecnologías *Wi-Fi* y *Bluetooth*, con las pruebas respectivas de transmisión de datos, se establece las siguientes conclusiones.

- Para interconectar redes punto a punto o multipunto, es más ventajoso la tecnología *Wi-Fi* que la *Bluetooth*, por su alcance, velocidad y desempeño, siendo recomendable en lugares en los que se necesite una red con dificultades para el cableado; por ejemplo al instalar una red tipo Ethernet.

La tecnología *Bluetooth* no tiene un gran desempeño en redes punto a punto LAN, debido a que esta tecnología esta orientada a conexión de dispositivos inalámbricos y transmisión de datos en pequeñas distancias (hasta 10metros con línea de vista), para mayores distancias se pierde la transmisión. *Bluetooth* esta siendo implementada actualmente en telefonía celular, dispositivos inalámbricos como: teclados, ratones, manos libres, impresoras, palms y también aparecer en los computadores personales.

Otro aspecto muy importante es la seguridad, la tecnología cuenta con protocolos en *Wi-Fi* cifrado *WEP, WPA, WPA2* y en *Bluetooth* claves *PIN* y seguridad *MAC*, para implementar seguridad los cuales de alguna forma nos brindan una solución. Las dos tecnologías brindan aspectos de seguridad limitados y quien las utiliza con información valiosa tendrá que implementar seguridad adicional.

RECOMENDACIONES

- Para proceder a la instalación de una red inalámbrica primero se tendría que realizar un estudio del ancho de banda necesario y la distancia que tendría que cubrir la red, para obtener el mayor beneficio de la tecnología utilizada.
- La tecnología Bluetooth va orientada en especial a la instalación de escritorios inalámbricos.
- Las especificaciones de la tecnología *Wi-Fi* son ideales para la instalación de una red inalámbrica LAN o WAN.
- El momento de adquirir los equipos se debe constatar las especificaciones técnicas del mismo, en cuanto a cobertura, velocidad y compatibilidad.
- Para el óptimo funcionamiento de las tecnologías inalámbricas es necesario tener instalado el Service Pack 2 para Windows.
- En ambientes industriales es común el monitoreo de muchos parámetros eléctricos o mecánicos donde Bluetooth puede formar una red de sensores de instrumentos de medida, removiendo las conexiones físicas entre estos y un centro de captura de datos, a esta red se le conoce como piconet. También permitirá la conexión, monitoreo y programación de controladores lógicos programables (*PLCs, PICs*) y puntos de campo instalados en líneas o plantas de producción.

GLOSARIO

3G	Redes amplias inalámbricas WWAN
AAA	Authentication Authorization Accounting
Access Point	Punto de acceso inalámbrico para conexión multipunto
Acknowledgement	Acuses de recibos
ACL	Asincrónico No Orientado a Conexión
ACO	Authenticated Ciphering Offset
	Proceso usado durante para la creación de la Clave de Cifrado
Active	Técnica a través de la cual ocurre la transmisión de datos en una conexión bluetooth
Ad Hoc o Peer to Peer	Dos o más clientes que son iguales entre ellos en una WLAN
AES	Advanced Encryption Standard
	Estándar avanzado de cifrado
AP	Access Point
ARQ	Automatic Repeat Request
	Protocolos de capa física
Barker	Clase de código para codificación de cada muestra
BD_ADDR	Dirección identificativa única del dispositivo Bluetooth
Beacons	Tipo de mensajes
Bluethoo	Tecnología que provee un camino fácil para la computación móvil
Browsing	Navegación
BSS	Basic Service Set
	Es el bloque básico de construcción de una LAN 802.11.
Btsockstat	Herramienta de diagnóstico interesante de alto nivel
Bytes	Unidad de almacenamiento de información conformada por 8 bits
CAM	Constant Awake Mode
	Modo de espera
CCMP	Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol
	Protocolo de cifrado de 802.11
Challenge-response	Procedimiento de autenticación
	Desafío-respuesta.
CMOS.	Complementary Metal Oxide Semiconductor
	Semiconductor complementario del óxido de metal
COF	Ciphering Offset
	Desplazamiento cifrado
CRC	Es el método que propone WEP para garantizar la integridad de los mensajes
CSMA/CA:	Carrier Sense Multiple Access / Collision avoidance
	Detección de acceso múltiple y control de colisiones
Discoverable mode	Dispositivo remoto
DS	Distribution System
	Arquitectura que se propone para interconectar distintos BSS
DSP	Digital Signal Processor
	Procesador de señales digitales

DSSS o FHSS o IR.	Modulación (propagación)
	Direct Sequence Spread Spectrum Para 2,4 GHz.
Duplex	Transmisión de datos de ambos sentidos
EAP	Protocolo de autentificación extensible para las tareas de autentificación, autorización, contabilidad
EAPOL	EAP over LAN
	EAP sobre LAN
ESS	Extended Service Set
	Wireless network de tamaño arbitrario
ESSID	Extended SSID
	SSID Extendido
FEC	Rate forward error correction
	Método diseñado para reducir el número de retransmisiones por errores
FHSS	Frequency Hopping Spread Spectrum
	Frecuencia que Brinca el Espectro del Cobertor
Firmware	Bloque de instrucciones de programa, grabado en una memoria tipo ROM,
FM	Frecuencia modulada
Frame body	Campo de datos
Frecuency hopping	Saltos de frecuencias
Full duplex	Transmisión de datos de ambos sentidos y simultáneamente
HCI	Interfaz de la Controladora de la Máquina
HEC	Header Error Control: CRC 32
	Cabecera de control de errores
Hola	Modo en el que no se requiere transmisión de datos entre el "master" o el "slave"
ICMP	Internet Control Message Protocol
	Protocolo de Control de Mensajes de Internet
IEEE	The Institute of Electrical and Electronics Engineers
	Instituto de Ingenieros Eléctricos y Electrónicos
802.11	Estándar de la tecnología Wi-Fi
Init	Inicio
Inquiry	Consulta
IP	Internet protocol
	Protocolo de Internet
IR	InfraRed
	Red infrarroja
ISM	Industrial, Scientific and Medical band.
	Banda de operación
IV	Initial vector
	Vector de inicio
Keystream	Generador de claves
L2CAP	Logical Link Control and Adaptation Protocol
Link Controller	Controlador de Enlace
Linkado	Enlazado
LLC:	Logical Link Control

LM	Link Manager
	Enlace principal
LMP	Link Manager Protocol
	Protocolo de enlace principal
LSFR	Linear Feedback Shift Registers
	Registros de desplazamiento retroalimentados
MAC:	Medium Access Control
	Control de acceso al medio
MAN	Metropolitan area Network
	Red de área metropolitana
Man in the Middle	Intruso
Master	Principal
Mbps	Mil bits por segundo
MIC	Message Integrity Code
	Código que verifica la integridad de los datos de las tramas.
Multiplexaje	Multiplexacion
OBEX	Objects Exchange Protocol
	Protocolo de intercambio de objetos
OSI	Open System Interconection
	Modelo de referencia de Interconexión de Sistemas Abiertos
OTP	One Time Password
	Contraseñas de un solo uso
Page/Inquiry	Dispositivo desea hacer una conexión con otro dispositivo
Pairing	Procedimiento de “pairing” cuando los dos dispositivos se comunican por primera vez.
Park	Escuchan para mantener su sincronización con el “master”
Payload	Carga útil de una trama
PDA	Personal Digital Assistant
	Es un computador de mano originalmente diseñado como agenda electrónica.
PDUs	Protocol Data Units
	Utiliza para el intercambio entre unidades pares, dentro una capa del modelo OSI
Piconet	Red de dispositivos informáticos que se conectan utilizando Bluetooth.
PIN	Clave
PLCP	Physical Layer Convergence Protocol
	Protocolo que se encarga de codificación y modulación en la capa física
PMD	Physical Médium Dependence
	Es la que crea la interfaz y controla la comunicación hacia la capa MAC
PPP	Point-to-Point Protocol
	Protocolo punto a punto
PRNG	Pseudo-Random Number Generador
	Numero generado randomicamente
QAM	Modulación en cuadratura de Fases con más de un nivel de amplitud
RADIUS	Remote Authentication Dial-In User Service
	Servidor AAA

RAND	Randómico
RC4	El algoritmo de encriptación
RF	Radio Frecuencia
RFCOMM	Protocolo utilizado para emular conexiones de puerto serial
RFCOMM.	El protocolo RFCOMM proporciona emulación de puertos serie a través del protocolo L2CAP
SAP:	Service Access Point
	Servicio de punto de acceso
Scatternet	la red producida cuando dos dispositivos pertenecientes a dos piconets diferentes, se conectan.
SCO	Síncrono Orientado a Conexión
SDP	Service Discovery Protocol
	Protocolo de Descubrimiento de Servicios
SIG	Special Interests Group
	Grupo de intereses especiales
Slave	Esclavo, secundario
Sniff:	Escucha a un reducido nivel.
SRES	Respuesta del demandante
SSID	Service Set identifiers
	Servicio de Identificación
Standby	Los dispositivos en un “piconet” que no están conectados, están en modo de espera
TCP	Transmission Control Protocol
	Protocolo de Control de Transmisión
TCS	Protocolo de control de telefonía
TKIP	Temporal Key Integrity Protocol
	El protocolo encargado de la generación de la clave para cada trama.
UDP	User Datagram Protocol
	Es un protocolo del nivel de transporte basado en el intercambio de datagramas.
UWB	Tipo de red inalámbrica
WEP	Wired Equivalent Privacy
	Privacidad equivalente al cable
Wi-Fi	Tecnología de red inalámbrica
WiMAX	Tecnología extendida de Wi-Fi
WLAN	Wireless local area network
	Red de área local inalámbrica
WMAN	Wireless metropolitan area network
	Red metropolitana inalámbrica
WPA	Wi-Fi Protected Access
	Acceso protegido Wi-Fi
WPAN	Wireless Personal Area Networks
	Red Inalámbrica de Área Personal
WWAN	Wirelees wide area networks
	Red inalámbrica de Amplio alcance
PLCs	Programador Lógico Controlable, utilizado para control automático de motores en procesos industriales
PICs	Circuitos Integrados Programables

BIBLIOGRAFIA

Curso Argentina WLAN, Ing. Martín Vernengo, mvernel@fi.uba.ar, 10/08/06.

Bluetooth, http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Conectar_el_PDA_al_PC_en_red_a_traves_de_Bluetooth.shtml, 05/08/06

Como configurar e Instalar Bluetooth, http://foro.todopocketpc.com/showthread.php?t=45463, 05/08/06

Tutoriales de telecomunicaciones, http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Conectar_el_PDA_al_PC_en_red_a_traves_de_Bluetooth.shtml, 05/08/06

Montar una Wlan, http://gsmlandia.com/instrucciones.php?instruccion_id=41,05/08/06

Problemas concretos de Seguridad en Wi-Fi en Curso de Seguridad en Wi-Fi (Técnico), http://www.wikilearning.com/problemas_concretos_de_seguridad_en_wifi-wkccp-4171-4.htm, Alejando Corletti Estrada, 14/08/06

Modelo de capas de 802.11 en Curso de Seguridad en Wi-Fi (Técnico), http://www.wikilearning.com/modelo_de_capas_de_802_11-wkccp-4171-2.htm, Alejando Corletti Estrada, 15/08/06

Tecnologías inalámbricas de banda ancha, http://www.intel.com/cd/network/communications/emea/spa/179913.htm 16/08/06

Antena - Wikipedia, la enciclopedia libre, http://es.wikipedia.org/wiki/Antena, 17/08/06

ZioShow.biz,

http://www.zioshow.biz/viewnews.php?id=449, ziogiorgio.biz, 18/08/06