BLUETOOTH.
APLICACIONES EN INSTRUMENTACIÓN INDUSTRIAL

EDUARDO CAMARGO DIAZGRANADOS
AMAURY DE JESUS OSORIO MEZA

Monografía presentada como requisito para obtener el titulo de Ingeniero Electrónico

Director
Ing. JORGE E. DUQUE

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA
PROGRAMA DE INGENIERIA ELECTRONICA
CARTAGENA DE INDIAS
2005

CONTENIDO

LISTA DE FIGURAS

Pag

LISTA DE TABLAS

Pag

1. INTRODUCCIÓN

Un bus de campo es un sistema de transmisión de información (datos) que simplifica enormemente la instalación y operación de máquinas y equipamientos industriales utilizados en procesos de producción. El objetivo de un bus de campo es sustituir las conexiones punto a punto entre los elementos de campo y el equipo de control a través del tradicional bucle de corriente de 4-20mA. Típicamente son redes digitales, bidireccionales, multipunto, montadas sobre un bus serie, que conectan dispositivos de campo como PLCs, transductores, actuadores y sensores. Cada dispositivo de campo incorpora cierta capacidad de proceso, que lo convierte en un dispositivo inteligente, manteniendo siempre un costo bajo. Cada uno de estos elementos será capaz de ejecutar funciones simples de diagnóstico, control o mantenimiento, así como de comunicarse bidireccionalmente a través del bus.

El objetivo es reemplazar los sistemas de control centralizados por redes de control distribuido mediante el cual permita mejorar la calidad del producto, reducir los costos y mejorar la eficiencia. Para ello se basa en que la información que envían y/o reciben los dispositivos de campo es digital, lo que resulta mucho más preciso que si se recurre a métodos analógicos. De esta forma, cada nodo de la red puede informar en caso de fallo del dispositivo asociado, y en general sobre cualquier anomalía asociada al dispositivo. Esta monitorización permite aumentar la eficiencia del sistema y reducir la cantidad de horas de mantenimiento necesarias.

En emplazamientos donde resulta complicado trazar un tendido de cable, es conveniente utilizar un enlace inalámbrico. Actualmente, este tipo de enlaces está

teniendo un gran auge debido a la aparición de sistemas de enlace como Wi-fi (IEEE 802.11b) y Bluetooth, que resuelven las comunicaciones entre dispositivos en distancias cercanas, pero donde se centran gran parte de las necesidades de los usuarios.

Bluetooth es un protocolo de comunicaciones inalámbrico de corto alcance y bajo consumo de potencia en la banda ICM de 2,4 GHz que soporta tanto tráfico de datos como de audio. Utiliza un sistema FH/TDD[1], en el que el canal queda dividido en intervalos de 625 µs, llamados slots, donde cada salto de frecuencia es ocupado por un slot. Esto da lugar a una frecuencia de salto de 1600 veces por segundo, en la que un paquete de datos ocupa un slot para la emisión y otro para la recepción y que pueden ser usados alternativamente, dando lugar a un esquema de tipo TDD. Su enlace es tan altamente confiable que hace de la tecnología una de las más aptas para cualquier tipo de aplicación en comunicaciones digitales, ya que habilita mecanismos de detección de error, ofrece una inmunidad natural a la interferencia empleando un espectro disperso de salto de frecuencia FHSS y habilita procesos de encriptación para garantizar comunicaciones confiables y seguras.

En ambientes industriales es común el monitoreo de muchos parámetros eléctricos o mecánicos donde Bluetooth puede formar una red de sensores e instrumentos de medida removiendo las conexiones físicas entre estos y un centro de captura de datos. Dos o más unidades Bluetooth pueden compartir el mismo canal dentro de una piconet, donde una unidad actúa como maestra, controlando el tráfico de datos en la piconet que se genera entre las demás unidades, donde estas actúan como esclavas, enviando y recibiendo señales hacia el maestro. El salto de frecuencia del canal está determinado por la secuencia de la señal, es decir, el orden en que llegan los saltos y por la fase de ésta secuencia. En Bluetooth, la secuencia queda fijada por la identidad de la unidad maestra de la piconet (un código único para cada equipo), y por su frecuencia de reloj. Por lo que, para que una unidad esclava pueda sincronizarse con una unidad maestra,

[1] FH/TDD: salto de frecuencia/división de tiempo duplex

ésta primera debe añadir un ajuste a su propio reloj nativo y así poder compartir la misma portadora de salto. A tal red se le conoce dentro de Bluetooth como *piconet*. También permitiría la conexión, monitoreo y programación de controladores lógicos programables PLCs, RTUs, y puntos de campo instalados en líneas o plantas de producción.

2. STACK DE PROTOCOLOS

El stack de protocolos de Bluetooth, al igual que todos los protocolos de este tipo, esta conformado por capas. Aunque no se conforma exactamente igual que el modelo de capas OSI, este expone el mismo comportamiento en él que al moverse de abajo hacia arriba, su implementación cambia gradualmente de hardware a firmware y finalmente a software. Si cada uno de este grupo de capas son entidades separadas, estas se pueden comunicar entre ellas a través de la HCI[2]. La HCI provee caminos para datos, audio, y señales de control entre el modulo Bluetooth y el host.

La radio completa la capa física suministrando un transmisor y receptor para la comunicación de dos vías. Los paquetes de datos son ensamblados y alimentados a la radio a través de la estación de banda base, este es el motor digital de un sistema Bluetooth. Es el responsable de construir y decodificar paquetes, codificar y administrar la corrección de errores, encriptación y des-encriptación para una comunicación segura, calcular los patrones de frecuencia para la transmisión por radio, mantener la sincronización, controlar la radio, y todos los demás detalles de bajo nivel necesarios para realizar la comunicación por Bluetooth.

El controlador de enlace provee operaciones de estado más complejas, tales como standby, conexión, y modos de baja potencia. Las funciones de banda base y controlador de enlace son combinadas en una capa como se ve en la figura 1.

El administrador de enlace provee control de enlace y configuración a través de un lenguaje de bajo nivel llamado protocolo administrador de enlace LMP[3], es el

[2] HCI: (Host Controller Interface – Interfase Controladora de Host)
[3] Por sus siglas en inglés (Link Manager Protocol)

responsable de crear y administrar el comportamiento del enlace inalámbrico en tiempo real, controlar el dispositivo de banda base y permitir el descubrimiento de servicio y por lo tanto establecer comunicación entre dos dispositivos Bluetooth y terminar el enlace con el comando o por error.

El protocolo de control y adaptación de enlace lógico, L2CAP[4] se sitúa encima de la capa HCI y provee control de flujo de datos y administración. Es el cerebro del sistema Bluetooth. Administra los aspectos de alto nivel de cada conexión (quién está conectado a quién, si usar encriptación o no, que nivel de rendimiento es requerido, etc.). Este establece canales virtuales entre hosts que pueden hacerle el seguimiento a varias sesiones simultáneas tal como la transferencia de múltiples archivos. L2CAP también toma los datos de aplicación y los fragmenta en pedazos de tamaño apropiado para la transmisión, y revierte el proceso para los datos recibidos. El L2CAP es implementado en software y se puede ejecutar ya sea en sistema procesador del host o en un procesador local en el sistema Bluetooth.

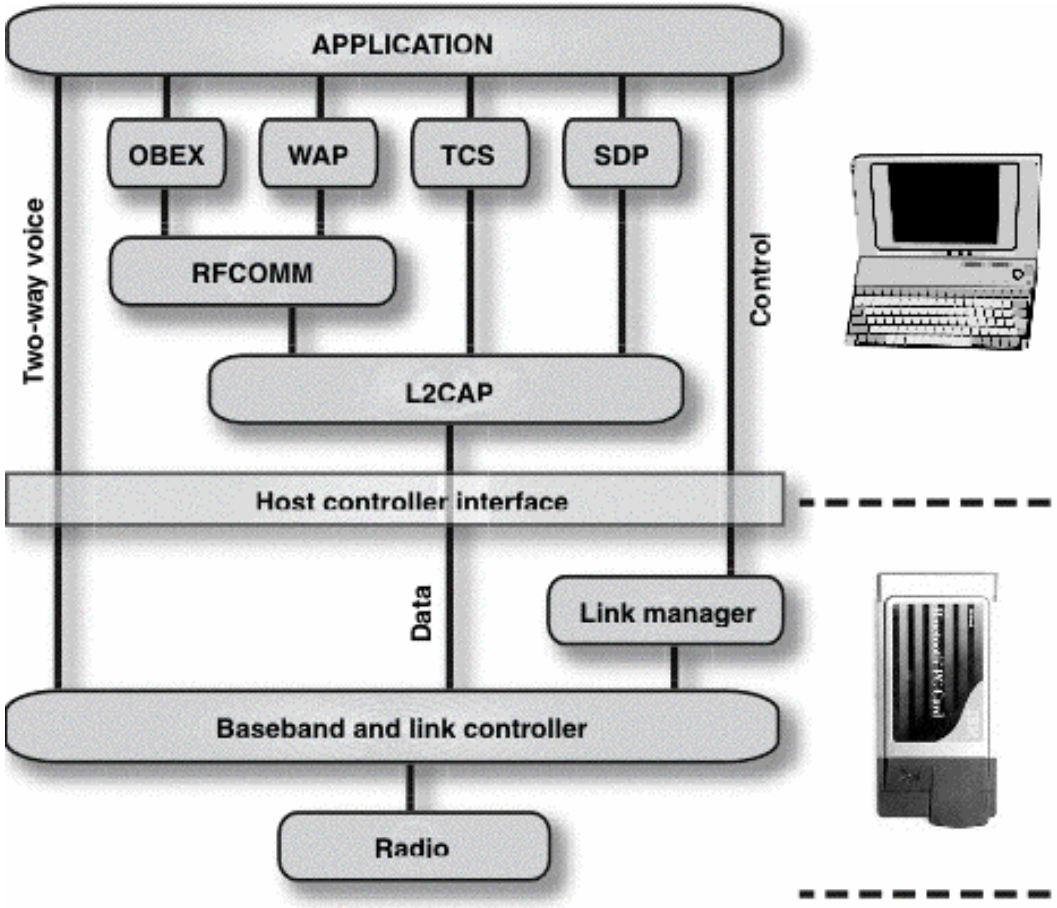
El RFCOMM[5], es el emulador de puerto serial de Bluetooth, y su propósito principal es engañar una aplicación para que piense que un puerto serial cableado existe en vez de un enlace RF. Finalmente, los programas que se necesitan para los diferentes modelos de uso de Bluetooth activan una aplicación familiar del Bluetooth. Estos incluyen SDP[6], OBEX[7], TCS[8], y WAP[9].

Aparte de comunicación de datos, Bluetooth tiene una provisión especial para voz digitalizada, en tiempo real y de dos vías. Una vez que estos paquetes son creados por una aplicación, omiten la mayor parte del stack de protocolos y son entregados directamente a la capa de banda base para prevenir retrasos inaceptables. El control del módulo Bluetooth generalmente procede de la

[4] Por sus siglas en ingles (Logical Link Control and Adaptation Protocol)
[5] RFCOMM: (Radio Frequency Communication - Comunicación de Radio Frecuencia)
[6] SDP: (Service Discovery Protocol – Protocolo para el Descubrimiento de Servicio)
[7] OBEX: (Object Exchange – Intercambio de Objetos)
[8] TCS: (Telephony Control Specifications – Especificaciones para el Control de Telefonía)
[9] WAP: (Wireless Application Protocol – Protocolo de Aplicación Inalámbrica)

aplicación a través del HCI al módulo, también pasando las capas de protocolo usadas para manejar el proceso de comunicación de datos.

Figura 1. Stack de Protocolos



3. ESPECIFICACIONES DE LA TECNOLOGÍA BLUETOOTH

3.1. ESPECIFICACIONES DE RADIO

3.1.1. Bandas De Frecuencia Y Canales

El sistema Bluetooth opera en la banda de 2.4 GHz, libre para ISM[10], en el rango entre 2400 y 2483.5 MHz. Algunos países, como España y Japón, tienen limitaciones en este rango de frecuencia por lo que se crearon algoritmos especiales de salto de frecuencia para estos, se producen 79 saltos en frecuencia desplazados 1 MHz. La frecuencia máxima de salto es de 1600 saltos por segundo.

Tabla 1. Bandas de frecuencias y canales

Geografía	Asignación Regulativa	Canales Bluetooth
USA	2.400 – 2.4835 GHz	f = 2402 + k MHz, k = 0…78
Europa	2.400 – 2.4835 GHz	f = 2402 + k MHz, k = 0…78
España	2.445 – 2.475 GHz	f = 2449 + k MHz, k = 0…22
Francia	2.4465 – 2.4835 GHz	f = 2454 + k MHz, k = 0…22
Japón	2.471 – 4.497 GHz	f = 2473 + k MHz, k = 0…22

Para cumplir con las regulaciones de fuera de banda en cada país, una banda guarda se utiliza en los bordes superior e inferior de la banda.

[10] ISM: (Industrial, Scientific, Medical)

Tabla 2. Bandas de guardas

Geografía	Banda Guarda Baja	Banda Guarda Alta
USA, Europa y casi todos los países	2 MHz	3.5 MHz

3.1.2. Características Del Transmisor

Los requisitos expresados en esta sección se dan como niveles de potencia en el conector de antena del equipo. Si el equipo no tiene un conector, una antena de referencia con ganancia de 0 dBi se asume.

El equipo se clasifica en tres clases según la potencia:

Tabla 3. Clasificación de equipos Bluetooth según la Potencia

Clase de Potencia	Máxima Potencia de Salida (Pmax)	Potencia de Salida Nominal	Potencia de Salida Mínima	Control de Potencia
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm a Pmax Optional: Pmin<-30 dBm a Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin<-30 dBm a Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin<-30 dBm a Pmax

Un control en la potencia se requiere para equipos de clase 1. Este control se utiliza para limitar la potencia transmitida sobre 0 dBm. La capacidad de control de potencia bajo 0 dBm es opcional y podría ser usada para optimizar el consumo de potencia y el nivel completo de interferencia. Los pasos de potencia formarán una secuencia monotonita, con un tamaño de paso máximo de 8 dB y un paso de

tamaño mínimo de 2 dB. Una equipo clase 1 con una transmisión de poder máxima de +20 dBm debe ser capaz de controlar su transmisión de apagado a 4 dBm o menos.

Un equipo con capacidad de control de potencia optimiza la potencia de salida en un enlace con comandos de LMP. Esto se logra midiendo el RSSI[11] y reportando si la potencia se debe aumentar o disminuir.

Note que la clase 1 no debe ser usada para enviar paquetes de un dispositivo a otro si el lado receptor de una conexión no soporta la mensajería necesaria para el control de potencia del lado transmisor. En este caso, el transmisor debe cumplir con las reglas de un transmisor clase 2 o clase 3.

También note que si un dispositivo clase 1 está paginando o pidiendo información muy cerca de otro dispositivo, la potencia de entrada podría ser mayor que lo requerido en el nivel utilizable máximo del receptor. Esto puede causar que el dispositivo que "escucha" falle al responder. Es por lo tanto útil paginar y preguntar usando la transmisión según las clases de poder 2 o 3.

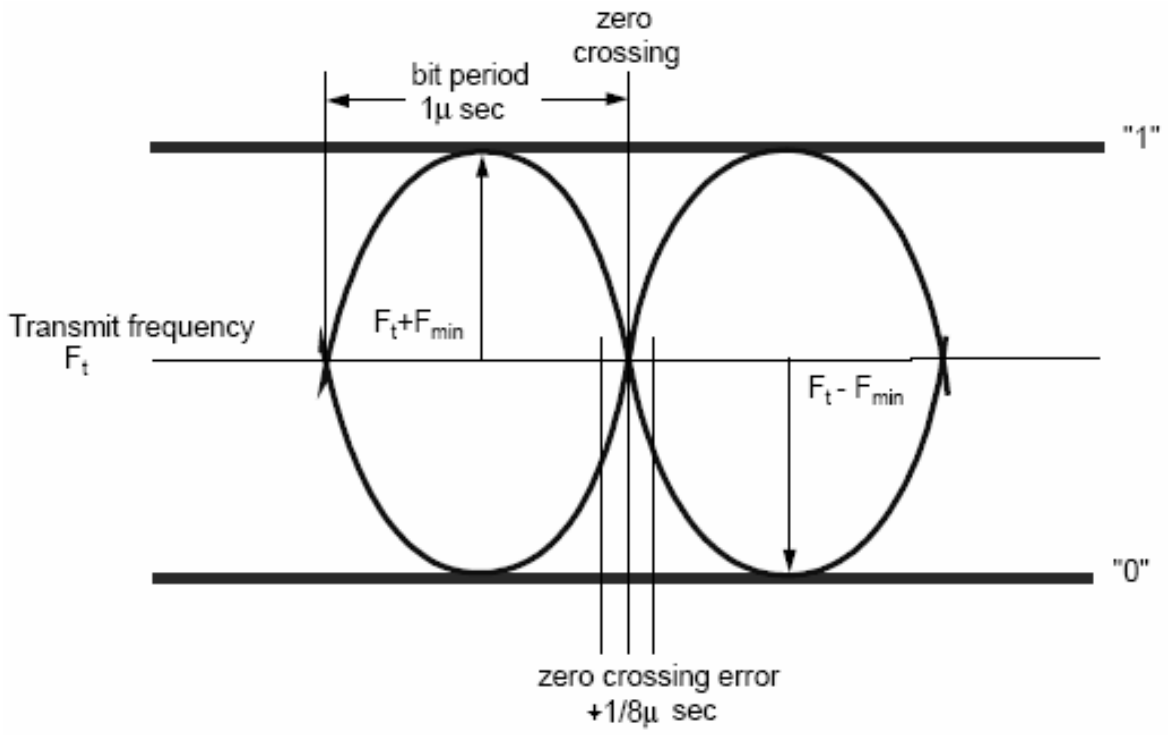
3.1.3. Características De Modulación

La Modulación es GFSK[12] con un BT[13] = 0,5. El índice de Modulación debe estar entre 0,28 y 0,35. Un uno binario es representado por una desviación positiva de la frecuencia portadora nominal, y un cero binario es representado por una desviación negativa de dicha frecuencia. El muestreo de símbolo deberá ser mejor que ±20 ppm.

Para cada canal de transmisión, la desviación mínima de la frecuencia (Fmin = el menor entre {Fmin +, Fmin-}) que corresponde a una secuencia 1010 no será menor al ±80% de la desviación de la frecuencia (fd) que corresponde a una secuencia 00001111.

[11] RSSI: (Receiver Signal Strength Indicator – Indicador de fuerza de la señal de receptor)
[12] GFSK: (Gaussian Frequency Shift Keying – Gaussiano por Corrimiento de Frecuencia)
[13] BT: (Bandwith Time – Tiempo de Ancho de Banda)

Figura 2. Modulación Gaussiana por corrimiento de frecuencia



Además, la desviación mínima nunca será más pequeña que 115 kHz. Los datos transmitidos tienen una tasa símbolo de 1 Ms/s.

El error de cruce por cero es la diferencia de tiempo entre el período ideal de símbolo y el tiempo de cruce medido. Esto será menor que ±1/8 de un período de símbolo.

Las emisiones falsas, en banda y fuera de banda, son medidas con un transmisor de salto de frecuencia saltando en una única frecuencia; esto significa que el sintetizador debe cambiar de frecuencia entre la ranura de recepción y la ranura de transmisión, pero siempre retorna a la misma frecuencia de transmisión.

La precisión de la frecuencia central inicial transmitida debe ser ±75 kHz desde Fc.

La exactitud de la frecuencia inicial está definida como la exactitud de la frecuencia antes de que cualquier información sea transmitida. Note que el requerimiento de movimiento de frecuencia no está incluido en los ±75 kHz.

El movimiento de la frecuencia central de un paquete en el transmisor está especificado en la Tabla 4.

Tabla 4. Movimiento de la frecuencia central de un paquete

Tipo de Paquete	Movimiento de Frecuencia
Paquete de un Slot	±25 kHz
Paquete de tres Slots	±40 kHz
Paquete de cinco Slots	±40 kHz
Máxima tasa de Movimiento	400 Hz/μs

3.1.4. Características Del Receptor

Para medir el desempeño de la tasa de error de bit; el equipo debe tener una facilidad de "retroalimentación". El equipo devuelve la información decodificada. El nivel de la sensibilidad de referencia es igual a -70 dBm.

Sensibilidad Real De Nivel

El nivel verdadero de sensibilidad se define como el nivel de entrada para el cual se logra una tasa de error de bit BER[14] no tratada de 0.1%. El requisito para un receptor Bluetooth es un nivel de sensibilidad verdadero de –70 dBm o mejor.

Desempeño De Interferencia

Los desempeños de interferencia en Canal Común y adyacente de 1 MHz y 2 MHz son medidos con la señal requerida 10 dB sobre el nivel de sensibilidad de referencia. En todas las otras frecuencias la señal requerida estará 3 dB sobre el nivel de sensibilidad de referencia. Si la frecuencia de una señal de interferencia se encuentra fuera de la banda de 2400-2497 MHz, la especificación de bloqueo de fuera de banda deberá ser aplicada. La señal de interferencia será modulada como Bluetooth. El BER será ≤0.1%. La razón señal a interferencia será:

[14] Por sus siglas en ingles (Bit Error Rate)

Tabla 5. Razón de la señal a interferencia

Requerimientos	Razón
Interferencia de Canal Común, $C/I_{canal\ común}$	11 dB
Interferencia Adyacente (1 MHz), $C/I_{1\ MHz}$	0 dB
Interferencia Adyacente (2 MHz), $C/I_{2\ MHz}$	-30 dB
Interferencia Adyacente (≥3 MHz), $C/I_{\geq 3\ MHz}$	-40 dB
Interferencia de Frecuencia Imagen, C/I_{Image}	-9 dB
Interferencia Adyacente (1 MHz) a frecuencia imagen dentro de banda, $C/I_{Image\pm 1MHz}$	-20 dB

Las frecuencias donde los requisitos no se reúnen se llaman frecuencias de respuesta falsa. Cinco frecuencias de respuesta falsa se permiten en frecuencias con una distancia de ≥2 MHz desde la señal deseada. En estas frecuencias de respuesta falsa deberá ser alcanzado un requisito de interferencia de estado estable C/I = -17 dB.

Bloqueo De Fuera De Banda

El bloqueo de fuera de banda es medido con la señal requerida 3dB por encima del nivel de sensibilidad de referencia. La señal de interferencia será una señal de onda continua. La BER será ≤ 0.1%. El bloqueo de fuera de banda deberá lograr los siguientes requerimientos:

Tabla 6. Bloqueo de fuera de banda

Frecuencia de la Señal de Interferencia	Nivel de Potencia de la Señal de Interferencia
30 MHz – 2000 MHz	-10 dBm
2000 – 2399 MHz	-27 dBm
2498 – 3000 MHz	-27 dBm
3000 MHz – 12.75 GHz	-10 dBm

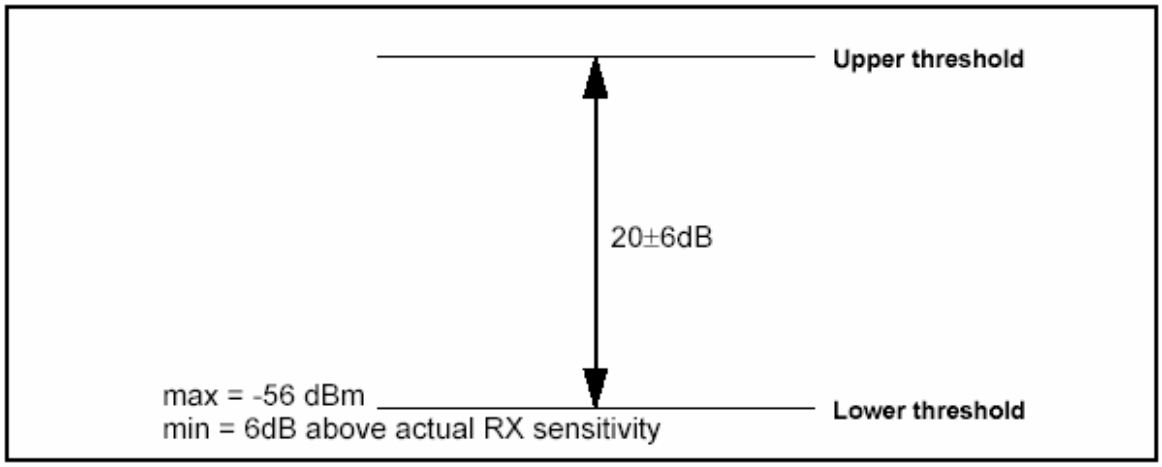
24 excepciones se permiten las cuales son dependientes sobre la frecuencia del canal de recepción dada y se centran en una frecuencia que es un múltiplo entero de 1 MHz.

Indicador De Fuerza De La Señal En El Receptor

Un receptor que desea soportar enlaces controlados de potencia debe ser capaz de medir la fuerza de la señal recibida y determinar si el transmisor en el otro lado del enlace debe aumentar o debe disminuir su nivel de potencia de salida. Un Indicador de Fuerza de la Señal (RSSI – Received Signal Strength Indicator) hace esto posible.

La medida de RSSI compara la potencia de la señal recibida con dos niveles umbrales. El nivel umbral más bajo corresponde a una potencia recibida entre -56 dBm y 6 dB sobre la sensibilidad real del receptor. El nivel umbral superior está 20 dB por encima del nivel umbral más bajo a una precisión de +/- 6 dB.

Figura 3. Niveles de umbrales de la medida RSSI



3.2. ESPECIFICACIONES DE BANDA BASE

3.2.1. Descripción General

Bluetooth es un enlace de radio de corto alcance hecho con la intención de reemplazar los cables que conectan dispositivos electrónicos portátiles y/o fijos.

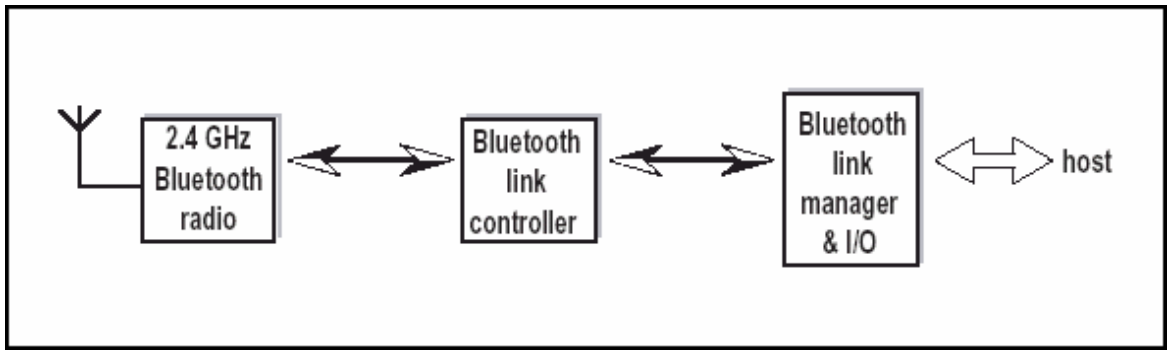
Las características clave son robustez, baja complejidad, bajo consumo, bajo costo.

Bluetooth opera en la banda sin licencia de 2.4 GHz. Se utiliza un transceptor con saltos de frecuencia para disminuir la interferencia y el fading[15]. Para minimizar la complejidad del transceptor se utiliza modulación FM binaria. La tasa de símbolo es de 1Ms/s. Se utiliza un canal ranurado con una duración de 625us. Para una transmisión duplex, se utiliza un esquema TDD[16]. En el canal, la información se intercambia en forma de paquetes. Cada paquete es transmitido en una frecuencia de salto diferente. Normalmente un paquete comprende una sola ranura, aunque puede ser extendido para abarcar hasta 5 ranuras de tiempo.

El protocolo utiliza una combinación de conmutación de circuitos y de paquetes. Las ranuras pueden estar reservadas para paquetes síncronos. Bluetooth soporta un canal de datos asíncronos, hasta 3 canales síncronos de voz simultáneos, o un canal que simultáneamente soporta datos asíncronos y voz síncrona. Cada canal de voz soporta una tasa de 64 kbps en cada dirección. El canal asíncrono puede soportar 723.2 kbps asimétricos o 433.9 kbps simétricos.

El sistema consiste en una unidad de radio, una unidad de control de enlace, y una de administración de enlace. En la Figura 4 se muestran los componentes de un sistema Bluetooth.

Figura 4. Componentes de un sistema Bluetooth

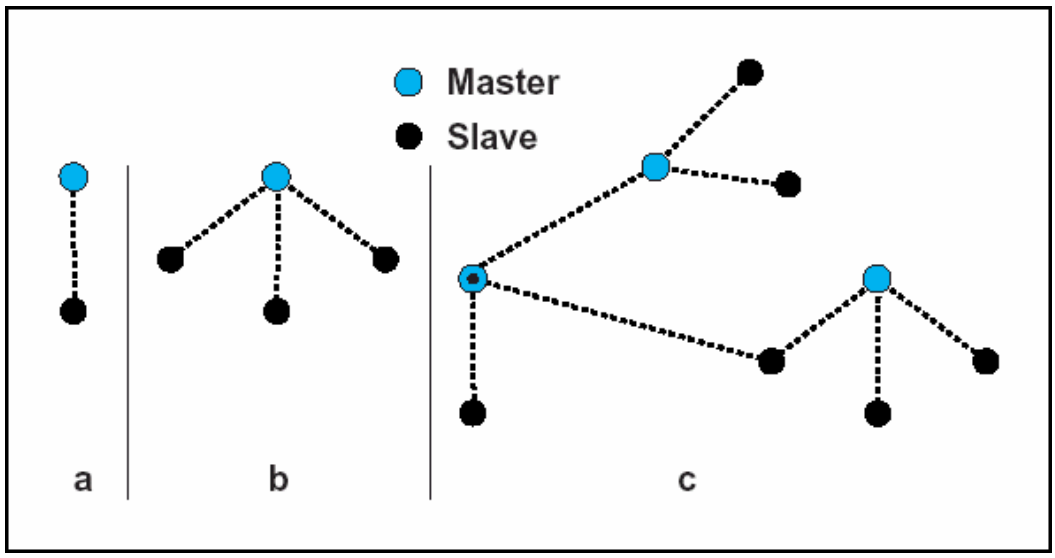


[15] Fading: Desvanecimiento de la Señal.
[16] Por sus siglas en ingles (Time-Division Duplex)

El sistema Bluetooth provee una conexión punto a punto, o punto a multipunto. En la conexión punto a multipunto, el canal es compartido entre varias unidades Bluetooth. Dos ó más unidades compartiendo el mismo canal forman una picored. Una unidad actúa como maestro de la red, mientras que el resto actúan como esclavas. Un maestro puede tener hasta siete esclavos activos en una picored. El canal es controlado por el maestro, un maestro también puede tener esclavos estáticos, no utilizan el canal de una manera activa pero siguen sincronizados con el maestro.

Múltiples picoredes con áreas que se superponen forman una scatternet[17]. Cada picored tiene un solo maestro, sin embargo los esclavos pueden participar en diferentes picoredes en una base de multiplexación por división de tiempo. Además, un maestro en una picored puede ser esclavo en otra. Las picoredes no estarán sincronizadas en frecuencia. Cada picored tiene su propia frecuencia de salto. En la Figura 5 se muestra un ejemplo de picoredes. En la parte A de la figura se muestra un maestro con un solo esclavo, en la parte B se muestra un maestro con 3 esclavos, mientras que en la C tenemos una scatternet con tres maestros siendo el de la izquierda un esclavo interconectando las otras dos redes.

Figura 5. Ejemplos de picoredes



[17] Scatternet: Diversas *picoredes* en donde sus rangos de cobertura se traslapan cuando dos dispositivos que pertenecen a picoredes diferentes, se conectan.

3.2.2. Canal Físico

Definición de Canal

El canal es representado por una secuencia de salto pseudo-aleatoria saltando a través de los 79 o 23 canales RF. La secuencia de salto es única para la picored y es determinada por la dirección del dispositivo Bluetooth maestro; la fase en la secuencia de salto es determinada por el reloj del maestro. El canal se divide en ranuras de tiempo donde cada ranura corresponde a una frecuencia de salto RF. Los saltos consecutivos corresponden a diferentes frecuencias de salto RF. La tasa nominal de salto es 1600 saltos/s. Todas las unidades Bluetooth participando en la picored están sincronizadas en tiempo y salto al canal.

Ranuras de Tiempo

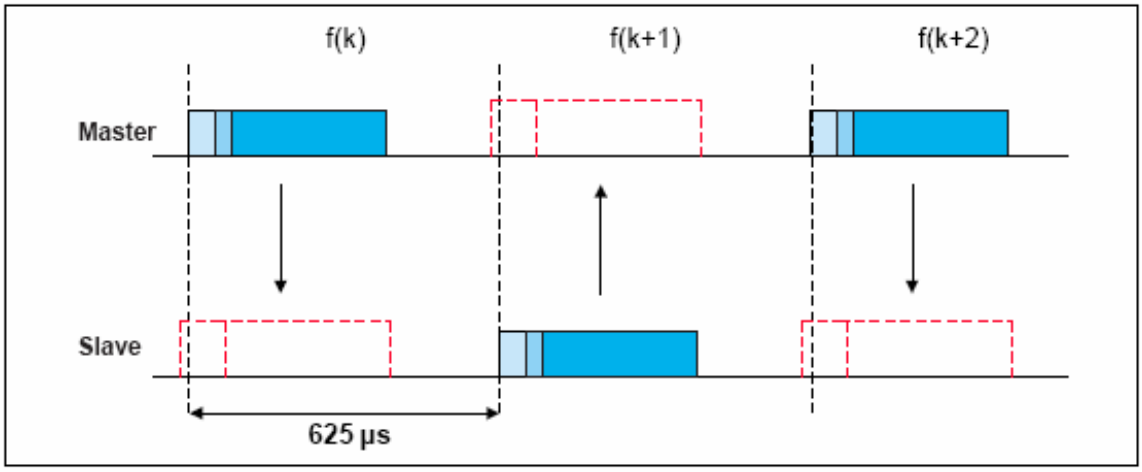
El canal se divide en ranuras de tiempo, cada una de 625μs de longitud. Las ranuras de tiempo se numeran según el reloj Bluetooth del maestro de la picored. La numeración de los rangos de las ranuras va desde 0 a 2^{27}-1 y es cíclica con una longitud de ciclo de 2^{27}.

En las ranuras de tiempo, el maestro y el esclavo pueden transmitir paquetes.

Se utiliza un esquema TDD, el maestro y el esclavo transmiten alternativamente como en la Figura 6. El maestro comenzará su transmisión en ranuras de tiempo pares solamente, y el esclavo comenzará su transmisión en ranuras de tiempo impares. El comienzo del paquete se alineará con el comienzo de la ranura. Los paquetes transmitidos por el maestro o el esclavo se pueden extender hasta cinco ranuras a la vez.

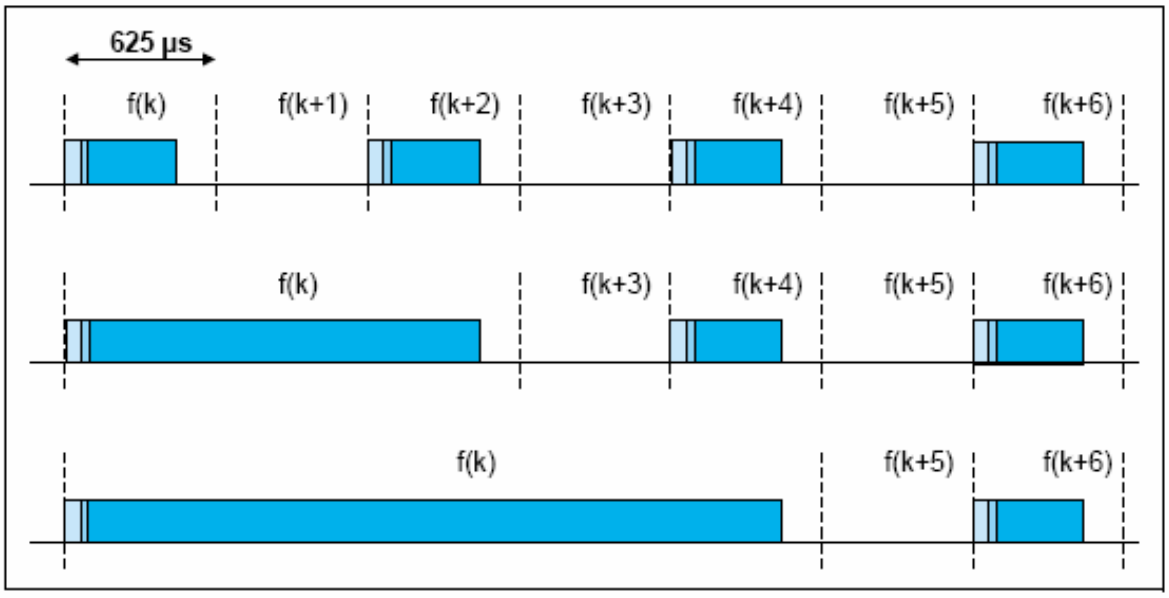
La frecuencia de salto RF permanecerá fija mientras dure el paquete. Para un solo paquete, la frecuencia de salto RF a ser usada es derivada del valor actual del reloj Bluetooth. Para un paquete multiranura, la frecuencia de salto RF a ser usada

Figura 6. Transmisión en una *piconet*.



por el paquete entero es derivada del valor de reloj Bluetooth en la primera ranura del paquete. La frecuencia de salto RF en la primera ranura después de un paquete multiranura usará la frecuencia como sea determinado por el valor actual del reloj Bluetooth. La Figura 7 ilustra la definición del salto en paquetes de una ranura y multiranura. Si un paquete ocupa más de una ranura de tiempo, la frecuencia de salto aplicada será la frecuencia de salto como fue aplicada en la ranura de tiempo donde la transmisión del paquete comenzó.

Figura 7. Salto en paquetes de una ranura y multiranura



3.2.3. Enlaces Físicos

General

Entre maestro y esclavo(s), se pueden establecer diferentes tipos de enlace. Se han definido dos tipos de enlace:

- Síncrono Orientado a la Conexión (SCO[18])
- Asíncrono no Orientado a la Conexión (ACL[19])

El enlace SCO es un enlace punto a punto entre un maestro y un solo esclavo en la picored. El maestro mantiene el enlace SCO usando ranuras reservadas en intervalos regulares. El enlace ACL es un enlace punto a multipunto entre el maestro y todos los esclavos que participan en la picored. En las ranuras no reservadas para el/los enlace(s) SCO, el maestro puede establecer un enlace ACL en una base por ranura a cualquier esclavo, incluyendo el/los esclavo(s) ya comprometido(s) en un enlace SCO.

Enlace SCO

El enlace SCO es un enlace simétrico, punto a punto entre el maestro y un esclavo específico. El enlace SCO reserva ranuras y por lo tanto puede ser considerado como una conexión por conmutación de circuito entre el maestro y el esclavo. El enlace SCO soporta típicamente información ligada al tiempo como la voz. El maestro puede soportar hasta tres enlaces SCO al mismo esclavo o a esclavos diferentes. Un esclavo puede soportar hasta tres enlaces SCO desde el mismo maestro, o dos enlaces SCO si los enlaces se originan de maestros diferentes. Los paquetes SCO nunca se retransmiten.

El maestro mandará paquetes SCO en intervalos regulares, el llamado intervalo SCO T_{SCO} (contado en ranuras) al esclavo en las ranuras maestro-esclavo reservadas. Al esclavo SCO siempre se le permite responder con un paquete SCO

[18] Por sus siglas en ingles (Synchronous Connection-Oriented)
[19] Por sus siglas en ingles (Asynchronous Connection-Less)

en la siguiente ranura maestro-esclavo a menos que el maestro se haya dirigido a un esclavo diferente en la ranura maestro-esclavo anterior. Si el esclavo SCO falla al decodificar la dirección de esclavo en el encabezamiento del paquete, se permite todavía devolver un paquete SCO en la ranura SCO reservada.

El enlace SCO es establecido por el maestro enviando un mensaje SCO de configuración por medio del protocolo administrador de enlace (LMP). Este mensaje contendrá los parámetros de tiempo tales como el intervalo SCO T_{SCO} y el offset D_{SCO} para especificar las ranuras reservadas.

Para prevenir los problemas de reloj, una bandera de inicialización en el mensaje LMP de configuración indica si se está utilizando el procedimiento de inicialización 1 o 2. El esclavo aplicará el método de inicialización indicado por la bandera de inicialización. El maestro utiliza inicialización 1 cuando el bit más significativo (MSB – Most Significant Bit) del reloj actual del maestro (CLK_{27}) es 0; usa la inicialización 2 cuando el MSB del reloj actual del maestro (CLK_{27}) es 1. Las ranuras SCO maestro-esclavo reservadas por el maestro y el esclavo se inicializarán en las ranuras para la cuál el reloj satisface la siguiente ecuación:

$CLK_{27-1} \bmod T_{SCO} = D_{SCO}$ para la inicialización 1

$(CLK_{27}, CLK_{26-1}) \bmod T_{SCO} = D_{SCO}$ para la inicialización 2

Las ranuras SCO esclavo-maestro seguirán directamente las ranuras SCO maestro-esclavo reservadas. Después de la inicialización, el valor de reloj CLK(k+1) para la próxima ranura SCO maestro-esclavo se encuentra agregando el intervalo fijo T_{SCO} al valor de reloj de la ranura SCO maestro-esclavo actual:

$$CLK(k+1) = CLK(k) + T_{SCO}$$

Enlace ACL

En las ranuras no reservadas para enlaces SCO, el maestro puede intercambiar paquetes con cualquier esclavo en una base por ranura. El enlace ACL

proporciona una conexión por conmutación de paquetes entre el maestro y todos los esclavos activos participando en la piconet. Ambos servicios, asíncronos e isócronos, son soportados. Entre un maestro y un esclavo sólo puede existir un enlace ACL. Para la mayoría de los paquetes ACL, reaplica la retransmisión de paquetes para asegurar la integridad de los datos.

Le es permitido a un esclavo devolver un paquete ACL en la ranura maestro-esclavo si y sólo recibió un paquete en la ranura maestro-esclavo anterior. Si el esclavo falla al decodificar la dirección de esclavo en el encabezamiento del paquete, no se le permite transmitir.

Los paquetes ACL no direccionados a un esclavo específico son considerados como paquetes broadcast[20] y son leídos por cada esclavo. Si no existen datos para ser enviados en el enlace ACL y ningún polling[21] es requerido, ninguna transmisión sucederá.

3.2.4. Paquetes

Formato General

El ordenamiento de bits cuándo se define paquetes y mensajes en las Especificaciones de Banda Base, siguen el formato de Pequeño Endian, en otras palabras, se aplican las siguientes reglas:

El Bit Menos Significativo (LSB – Less Significant Bit) corresponde a b_0;

El LSB es el primer bit transmitido;

En ilustraciones, el LSB se muestra en el lado izquierdo;

El controlador de enlace interpreta el primer bit llegando de una capa más alta de software como b_0; en otras palabras esto es el primer bit para ser transmitido.

[20] Los paquetes **broadcast** son paquetes transmitidos desde el maestro a todos los esclavos.

[21] Polling: Proceso de interrogación cíclico.

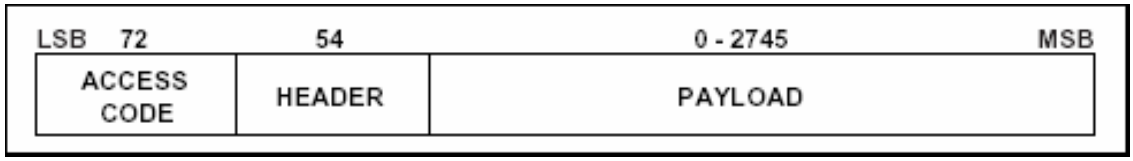
Además, los campos de datos generados internamente en el nivel de banda base, tal como los campos de encabezamiento del paquete y la longitud del encabezamiento de la carga útil, se transmiten primero con el LSB. Por ejemplo, un parámetro de 3 bits X = 3 es transmitido como:

$b_0\ b_1\ b_2 = 110$

Donde los 1 se transmiten primero y los 0 de último.

Los datos en el canal de la picored se transmiten en paquetes. El formato general del paquete se muestra en la Figura 8. Cada paquete se compone de 3 entidades: el código del acceso, el encabezamiento, y la carga útil. En la figura, el número de bits por entidad se indica.

Figura 8. Formato de paquete general



El código de acceso y el encabezamiento son de tamaño fijo: 72 bits y 54 bits respectivamente. La carga útil puede estar en el rango desde cero a un máximo de 2745 bits. Se han definido diferentes tipos de paquetes. Los paquetes pueden estar formados por el código de acceso (reducido) solamente, por el código de acceso y el encabezamiento, o por el código de acceso, el encabezamiento y la carga útil.

Código de Acceso

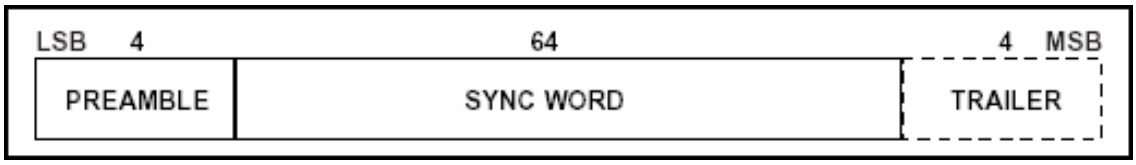
Cada paquete comienza con un código de acceso. Si sigue un encabezamiento de paquete, el código de acceso es de 72 bits, de otro modo el código de acceso es de 68 bits. Este código de acceso se usa para la sincronización, la compensación

del offset[22] en DC y para la identificación. El código de acceso identifica todos los paquetes intercambiados en el canal de la piconet: todos los paquetes enviados en la misma piconet son precedidos por el mismo código de acceso del canal. En el receptor de la unidad Bluetooth, un correlacionador deslizante correlaciona contra el código de acceso y se dispara cuando un umbral se excede. Esta señal del disparador se usa para determinar la sincronización de recepción.

El código de acceso también es utilizado en procedimientos de llamada y consulta. En este caso, el mismo código de acceso es utilizado como un mensaje de señalización y ni un encabezamiento ni una carga útil están presentes.

El código del acceso consiste en un preámbulo, una palabra de sincronización, y posiblemente un trailer, vea la Figura 9.

Figura 9. Formato del código del acceso



Tipos de Código de Acceso

Existen tres tipos diferentes de códigos de acceso definidos:

- Código de Acceso de Canal (CAC – Channel Access Code)
- Código de Acceso de Dispositivo (DAC – Device Access Code)
- Código de Acceso de Consulta (IAC – Inquiry Access Code)

Los tipos de código de acceso respectivos se usan para una unidad Bluetooth en modos de operación diferentes. El código de acceso de canal identifica una piconet. Este código incluye todos los paquetes intercambiados en el canal de la piconet. El código de acceso del dispositivo es utilizado para procedimientos especiales de señalización, por ejemplo, llamada y la respuesta a llamada. Para el

[22] Offset: Desplazamiento.

código de acceso de consulta hay dos variaciones. Un código de acceso de consulta general (GIAC[23]) es común a todos los dispositivos. El GIAC puede ser utilizado para descubrir si otras unidades Bluetooth están dentro del rango. El código de acceso de consulta dedicado (DIAC[24]) es común para un grupo dedicado de unidades Bluetooth que comparten una característica común. El DIAC se puede utilizar para descubrir sólo estas unidades Bluetooth dedicadas dentro del rango.

El CAC consiste en un preámbulo, una palabra de sincronización, y el trailer, y su longitud total es de 72 bits. Cuando se utiliza como mensaje auto-contenido sin un encabezamiento, el DAC y IAC no incluyen los bits de trailer y son de una longitud de 68 bits.

Los diferentes tipos de código de acceso utilizan Partes de Direcciones Bajas (LAPs[25]) diferentes para construir la palabra de sincronización. Un resumen de los diferentes tipos de código de acceso se puede encontrar en la Tabla 7.

Tabla 7. Tipos de código de acceso

Tipo de Código	LAP	Longitud de Código
CAC	Maestro	72
DAC	Unidad Llamada	68/72
GIAC	Reservada	68/72
DIAC	Dedicada	68/72

Preámbulo

El preámbulo es un patrón fijo de ceros y unos, de 4 símbolos, utilizado para facilitar la compensación DC. La sucesión es o 1010 o 0101, dependiendo si el LSB de la siguiente palabra de sincronización es 1 o 0, respectivamente. El preámbulo se muestra en la Figura 10.

[23] GIAC: por sus siglas en ingles (General Inquirí Access Code)
[24] DIAC: por sus siglas en ingles (Dedicated Inquiry Access Code)
[25] LAPs: por sus siglas en ingles (Lower Address Parts)

Figura 10. Formato del preámbulo

Palabra de Sincronización

La palabra de sincronización es una palabra código de 64 bits derivada de una dirección (LAP) de 24 bits; para el CAC se utiliza el LAP del maestro; para el GIAC y el DIAC, se utilizan LAPs reservados y dedicados; para el DAC, se utiliza el LAP de la unidad esclavo. La construcción garantiza una gran distancia Hamming[26] entre palabras de sincronización basadas en LAPs diferentes. Además, las buenas propiedades de auto-correlación de la palabra de sincronización mejoran el proceso de sincronización de los tiempos.

Trailer

El trailer[27] es añadido a la palabra de sincronización tan pronto como el encabezamiento del paquete sigue el código de acceso. Esto es típicamente el caso con el CAC, pero el trailer se usa también en el DAC y el IAC cuando estos códigos son usados en paquetes FHS intercambiados durante los procedimientos de respuesta de llamada y respuesta de consulta.

El trailer es un patrón fijo de ceros y unos de cuatro símbolos. El trailer junto con los tres MSBs de la palabra de sincronismo forma un patrón de 7 bits de unos y ceros alternados que se pueden usar para la compensación DC extendida. La secuencia del trailer es o 1010 o 0101 dependiendo de si el MSB de la palabra de sincronización es 0 o 1, respectivamente. La elección de trailer se ilustra en la Figura 11.

[26] Código Hamming: Los *bits* de información son agrupados en secuencias de 10 *bits*, éstos son enviados como 15 *bits* y el algoritmo corrige todos los errores de un *bit* y detecta los errores de dos *bits.*
[27] Trailer: Avance.

Figura 11. Formato del trailer

Encabezamiento del Paquete

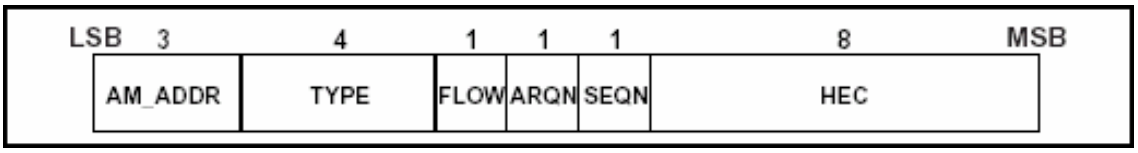
El encabezamiento contiene información de control de enlace (LC – Link Control) y consiste en 6 campos:

- **AM_ADDR** (Active Member Address): Dirección de miembro activo de 3-bits. El AM_DDR representa la dirección de un miembro de la piconet y se utiliza para distinguir entre los miembros activos de esta. En una piconet, uno o más esclavos están conectados a un único maestro. Para identificar cada esclavo por separado, a cada uno se le asigna una dirección temporal de 3 bits para ser usada cuando esté activo.
- **TYPE**: Código de tipo de 4-bit. Se pueden distinguir 16 tipos diferentes de paquetes. Este código especifica el tipo de paquete utilizado. Además también revela cuantas ranuras ocupa el paquete actual.
- **FLOW**: Control de flujo de 1-bit. Este bit se utiliza para control de flujo de paquetes sobre el enlace ACL.
- **ARQN**: Indicación de reconocimiento de 1-bit. Es utilizado para informar a la fuente de una transferencia exitosa de datos de carga útil con un chequeo de redundancia cíclica (CRC – Cyclic Redundancy Check), y puede ser de reconocimiento positivo (ACK) o de reconocimiento negativo (NAK).
- **SEQN**: Número de secuencia de 1-bit. Provee un esquema secuencial numerado para ordenar los de paquetes de datos. Por cada nuevo paquete transmitido que contiene datos con CRC, el bit SEQN se invierte. Esto se requiere para filtrar retransmisiones en el destino.

- **HEC**: Chequeo de error de encabezamiento de 8-bits. Cada encabezamiento tiene un HEC para chequear la integridad de este. Consiste en una palabra polinomial de 8 bits.

El encabezamiento total, incluyendo el HEC, se compone de 18 bits, vea la Figura 12, y es codificado con una tasa 1/3 FEC[28] lo que resulta en un encabezamiento de 54 bits.

Figura 12. Formato de cabecera de paquete



3.2.5. Corrección De Errores

Existen tres esquemas de corrección de error definidos para Bluetooth:

• FEC con tasa de 1/3
• FEC con tasa de 2/3
• Esquema ARQ para los datos

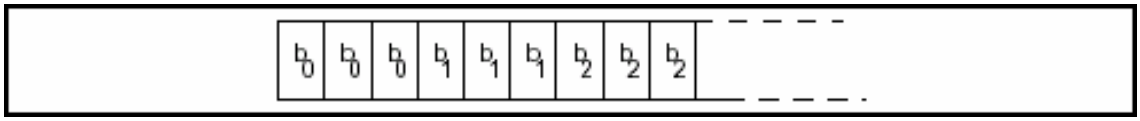
El propósito del esquema FEC en la carga útil de datos es reducir el número de retransmisiones. Sin embargo, en un ambiente razonable libre de errores, FEC reduce el rendimiento. El encabezamiento del paquete siempre es protegido por FEC con tasa de 1/3; contiene información valiosa del enlace y debe ser capaz de soportar más errores de bit.

Código FEC: Tasa de 1/3

Un simple código FEC de 3 repeticiones se utiliza para el encabezamiento. El código de repetición se implementa repitiendo tres veces el bit; vea la ilustración en la Figura 13.

[28] FEC: (Forward Error Correction code – Código de Corrección de Error en Adelanto)

Figura 13. Código FEC



Código FEC: Tasa de 2/3

En la carga útil se usa un esquema de código Hamming. Los bits de información son agrupados en secuencias de 10 bits, éstos son enviados como 15 bits y el algoritmo corrige todos los errores de un bit y detecta los errores de dos bits.

Esquema ARQ

Para garantizar una recepción correcta, todos los paquetes de datos son retransmitidos hasta que el emisor reciba una confirmación. La confirmación es enviada en la cabecera de los paquetes retornados. Para determinar si la carga útil es correcta o no, un código de chequeo de redundancia cíclica (CRC[29]) se añade al paquete. El esquema ARQ sólo trabaja en la carga útil del paquete (sólo esa carga útil que tiene un CRC). El encabezamiento del paquete y la carga útil de voz no son protegidos por el esquema de ARQ.

Para asegurar que no desaparezcan paquetes completos, Bluetooth usa números de secuencia. Actualmente sólo se usa un número de secuencia de un bit.

Un ACK (ARQN=1) o un NAK (ARQN=0) es devuelto en respuesta al recibo del paquete previamente recibido. El esclavo responderá en la ranura esclavo-maestro directamente siguiente de la ranura maestro-esclavo.

Paquetes de Broadcast.

Los paquetes broadcast son paquetes transmitidos desde el maestro a todos los esclavos. No hay posibilidad de usar confirmación para esta comunicación, sin

[29] CRC: por sus siglas en ingles (Cyclic Redundancy Check)

embargo, para incrementar la posibilidad de recibir correctamente un paquete, cada *bit* en el paquete es repetido un número fijo de veces.

3.2.6. Rutinas De Transmisión /Recepción

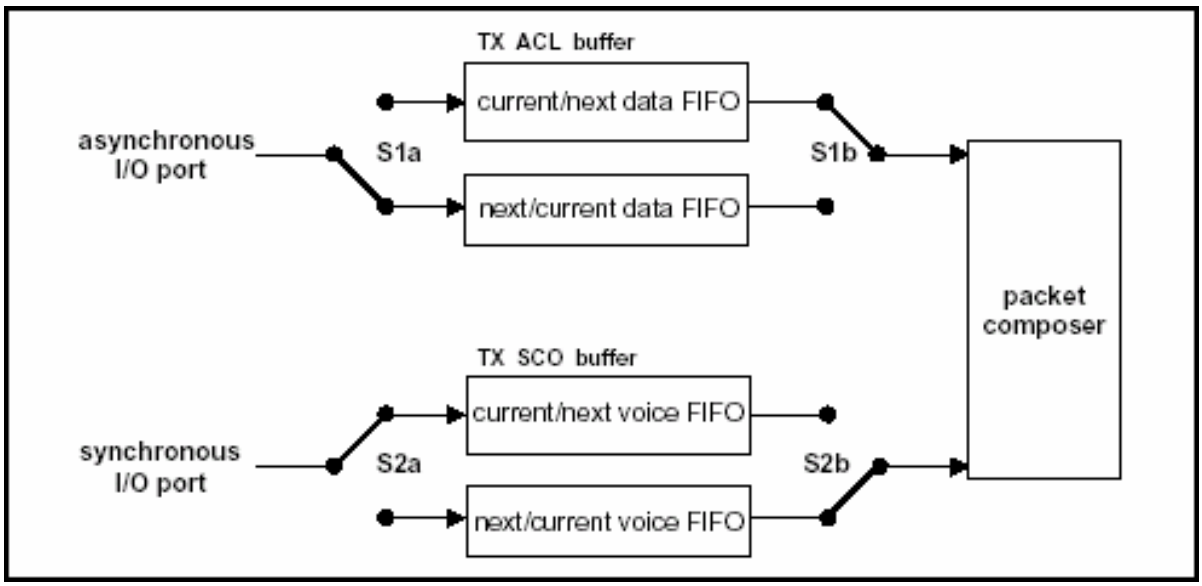
Rutina T_X

La rutina de T_X se lleva a cabo por separado para cada enlace ACL y cada enlace SCO. La Figura 14 muestra los búferes ACL y SCO al ser utilizados en la rutina de T_X. En esta figura, se muestran sólo un solo búfer de T_X ACL y un solo búfer de T_X SCO. En el maestro, hay un búfer de T_X ACL separado para cada esclavo. Puede haber además uno o más búferes de T_X SCO por cada esclavo SCO (enlaces SCO diferentes pueden o reutilizar el mismo búfer de T_X SCO, o cada uno tiene su propio búfer de T_X SCO). Cada búfer de T_X se compone de dos registros FIFO: un registro actual que puede ser accedido y leído por el controlador Bluetooth para componer los paquetes, y un registro siguiente que puede ser accedido por el Administrador de Enlace Bluetooth para cargar información nueva. Las posiciones de los interruptores S1 y S2 determinan cuál registro es actual y cuál registro es siguiente; los interruptores son controlados por el Administrador de Enlace Bluetooth. Los interruptores en la entrada y la salida de los registros FIFO nunca pueden ser conectados al mismo registro simultáneamente.

Como se mencionó antes, el maestro de la piconet empieza enviando en ranuras de tiempo pares y el esclavo en las impares. Sólo el último esclavo direccionado está autorizado para enviar en la ranura de tiempo de los esclavos. Esto no causa problemas ya que el maestro siempre está inicializando todas las conexiones y transmisiones nuevas. Cada esclavo espera las oportunidades de conexión dadas por el maestro. Los paquetes pueden ser más grandes que una ranura de tiempo, debido a esto el maestro puede continuar enviando en las ranuras de tiempo impares y viceversa. El sistema de reloj del maestro sincroniza a toda la piconet. El maestro nunca ajusta su sistema de reloj durante la existencia de una piconet, son los esclavos quienes adaptan sus relojes con un offset de tiempo con el fin de

igualarse con el reloj del maestro. Este offset es actualizado cada vez que es recibido un paquete desde el maestro.

Figura 14. Búferes de ACL y SCO en la transmisión



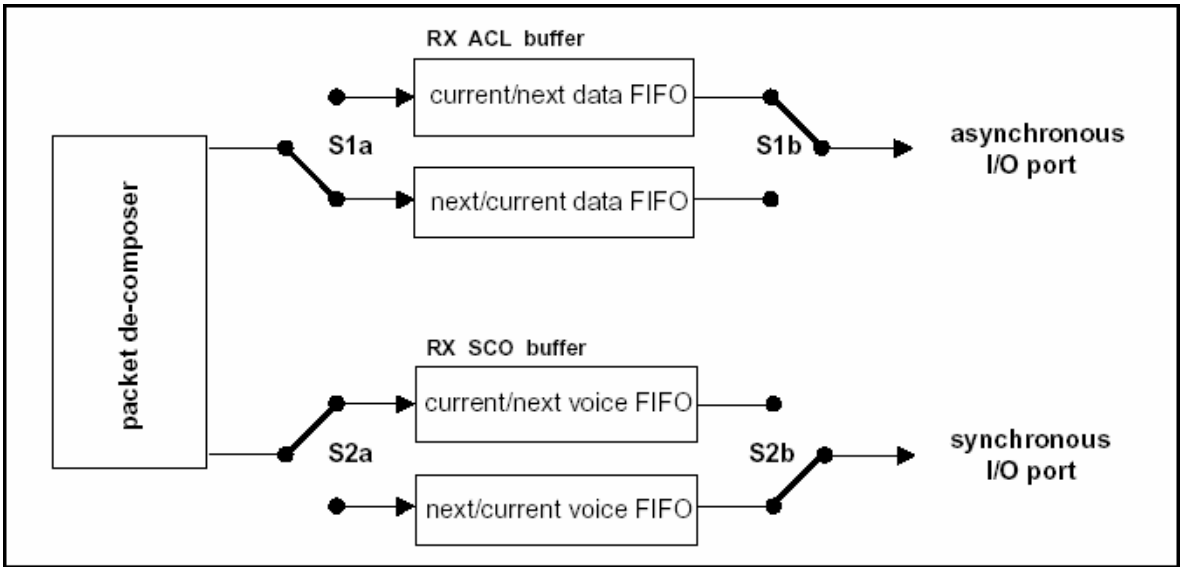
Rutina Rx

La rutina Rx se lleva a cabo por separado para el enlace ACL y el enlace SCO. Sin embargo, un solo búfer Rx se comparte entre todos los esclavos. La Figura 15 muestra los búferes ACL y SCO como se utilizan en la rutina Rx. El búfer ACL Rx consiste en dos registros FIFO: un registro que puede ser accedido y cargado por el controlador de enlace de Bluetooth con la carga útil del último paquete Rx, y un registro que puede ser accedido por el Administrador de enlace de Bluetooth para leer la carga útil anterior. El búfer SCO Rx también consiste en dos registros FIFO: un registro que se llena con información de voz recién llegada, y un registro que puede ser leído por la unidad procesadora de voz.

3.2.7. Seguridad En Bluetooth

Con el fin de brindar protección y confidencialidad a la información, el sistema debe ofrecer medidas de seguridad en las dos capas, la de aplicación y la de

Figura 15. Búferes de ACL y SCO en la recepción



enlace. Todas las unidades Bluetooth tienen implementadas las mismas rutinas de autenticación y encriptación. En la capa de enlace, estas rutinas constan de cuatro entidades diferentes: una dirección pública que es única para cada usuario, dos llaves secretas y un número aleatorio el cual es diferente para cada transacción. Solamente es encriptada la carga útil. El código de acceso y la cabecera de paquete nunca son encriptados. A continuación se muestra una tabla con las 4 entidades y su longitud:

Tabla 8. Entidades de la capa de enlace

Entidad	Tamaño
BD_ADDR	48 bits
Llave privada de usuario, autenticación	128 bits
Llave privada de usuario, encriptado de longitud configurable	8 - 128 bits
RAND	128 bits

La dirección del dispositivo Bluetooth (BD_ADDR – Bluetooth Device Address) es la dirección de 48 bits que es única para cada unidad Bluetooth. Las direcciones Bluetooth son públicas, y pueden ser obtenidas por medio de interacciones MMI, o, automáticamente, vía una rutina de indagación por una unidad Bluetooth.

Las llaves secretas se derivan durante la inicialización y nunca más son reveladas. Normalmente, la llave de encriptación se deriva de la llave de autenticación durante el proceso de autenticación. Para el algoritmo de autenticación, el tamaño de la llave usada es siempre 128 bits. El maestro genera un número aleatorio y lo envía al esclavo, el esclavo usa este número y su propia identidad para calcular el número de autenticación. Luego, este número es enviado al maestro quien hace el mismo cálculo. Si los dos números generados son iguales entonces la autenticación es concedida. Para el algoritmo de encriptación, el tamaño de la llave puede variar entre 1 y 16 octetos (8 - 128 bits). El tamaño de la llave de encriptación será configurable por dos razones. Primero por los muchos requisitos diferentes impuestos en algoritmos cifrados en diferentes países. La segunda razón es para facilitar una futura vía de actualización para la seguridad sin la necesidad de un costoso rediseño del hardware de algoritmos y encriptación Actualmente parece que el tamaño de la llave de encriptación de 64 bits proporciona protección satisfactoria para la mayoría de las aplicaciones.

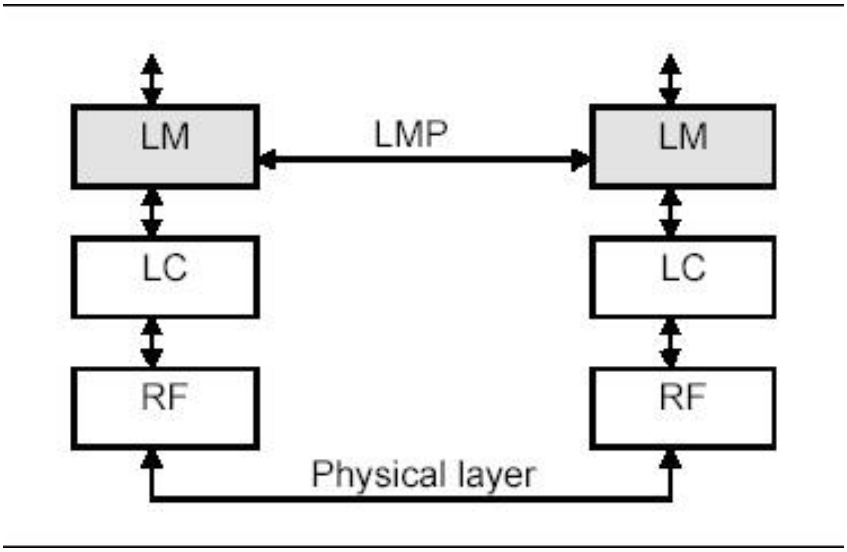
El RAND es un número aleatorio que se puede derivar de un proceso aleatorio o pseudo-aleatorio en la unidad Bluetooth. Esto no es un parámetro constante, cambiará frecuentemente.

3.3. PROTOCOLO DE GESTIÓN DE ENLACE (LMP – LINK MANAGER PROTOCOL)

3.3.1. General

Los mensajes LMP se utilizan para el establecimiento, seguridad y control del enlace. Estos son transferidos en la carga útil en vez de los mensajes de datos de L2CAP y se distinguen por un valor reservado en el campo L_CH del encabezamiento de la carga útil. Los mensajes se filtran e interpretan por el administrador de enlace en el lado receptor y no son propagados a capas más altas.

Figura 16. Flujo de los mensajes LMP



Los mensajes del Administrador de Enlace tienen una prioridad más alta que los datos de usuario. Esto significa que si el Administrador de Enlace necesita enviar un mensaje, no será retrasado por el tráfico L2CAP, aunque puede ser retrasado por muchas retransmisiones de paquetes individuales de banda base.

3.3.2. Formato Del LMP

Los PDU LM son siempre enviados como paquetes de ranura única y el encabezamiento de la carga útil es por lo tanto un byte. Los dos bits menos significativos en el encabezamiento de la carga útil determinan el canal lógico. Para los PDU LM estos bits fijados son.

Tabla 9. Bits fijos de los PDU LM

L_CH Code	Canal Lógico	Información
00	NA	Indefinido
01	UA/I	Continuando mensaje L2CAP
10	UA/I	Comienza mensaje L2CAP
11	LM	Mensaje L2CAP

El bit de FLUJO en el encabezamiento de la carga útil es siempre uno y se ignora en el lado receptor. A cada PDU se le asigna un opcode[30] de 7 bits utilizado para identificar de manera única los tipos diferentes de PDUs. El opcode y una identificación de transacción de un bit se posicionan en el primer byte del cuerpo de la carga útil. La identificación de transacción se posiciona en el LSB. Es 0 si el PDU pertenece a una transacción iniciada por el maestro y 1 si el PDU pertenece a una transacción iniciada por el esclavo. Si el PDU contiene uno o más parámetros éstos se colocan en la carga útil que comienza en el segundo byte del cuerpo de la carga útil.

La fuente/destino de los PDUs es determinada por el AM_ADDR en el encabezamiento del paquete.

3.3.3. PDUs Y Reglas De Procedimiento

Cada procedimiento se describe y es representado con un esquema de secuencia. Los símbolos siguientes se utilizan en los esquemas de secuencia:

El PDU1 es un PDU enviado de A a B. El PDU2 es un PDU enviado de B a A. El PDU3 es un PDU que se opcionalmente enviado de A a B. El PDU4 es un PDU opcionalmente enviado de B a A. El PDU5 es un PDU enviado de A o B. Una línea vertical indica que más PDUs se pueden enviar opcionalmente.

Mensajes de Respuesta General

Los PDUs LMP_aceptado y LMP_no_aceptado son usados como mensajes de respuesta a otros PDUs en varios procedimientos diferentes. El PDU LMP_aceptado incluye el opcode del mensaje que se acepta. El PDU LMP_no_aceptado incluye el opcode del mensaje que no se acepta y la razón por la qué no se acepta.

[30] Opcode: código e operación

Figura 17. Procedimiento de las PDUs

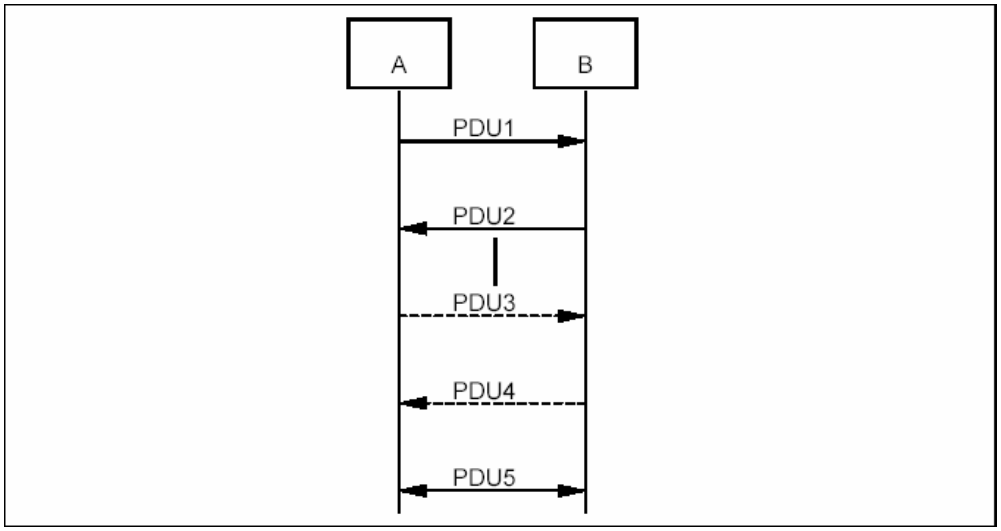


Tabla 10. Mensaje de respuesta general

M/O	PDU	Contenido
M	LMP_aceptado	op code
M	LMP_no_aceptado	op code reason

Autenticación

El procedimiento de autenticación se basa en un esquema de desafío-respuesta. El verificador envía un PDU LMP_au_rand que contiene un número aleatorio (el desafío) al solicitante. El solicitante calcula una respuesta, que es una función del desafío, el BD_ADDR del solicitante y una llave secreta. La respuesta es devuelta al verificador, que chequea si la respuesta era correcta o no. Un cálculo exitoso de la respuesta de autenticación requiere que dos dispositivos compartan una llave secreta. Ambos el maestro y el esclavo pueden ser verificadores. Los siguientes PDUs se utilizan en el procedimiento de autenticación:

Tabla 11. PDUs de autenticación

M/O	PDU	Contenido
M	LMP_au_rand	Número aleatorio
M	LMP_sres	Respuesta de autenticación

Paridad

Cuándo dos dispositivos no tienen una llave de enlace común una llave de inicialización (Kinit) se crea basada en un número de identificación personal (PIN[31]), un número aleatorio y una dirección de un dispositivo Bluetooth (BD – Bluetooth Device). Cuándo ambos dispositivos han calculado K_{init} la llave de enlace se crea, y finalmente un autenticación mutua se realiza. Los PDUs utilizados en el procedimiento de paridad son:

Tabla 12. PDUs de paridad

M/O	PDU	Contenidos
M	LMP_in_rand	Número aleatorio
M	LMP_au_rand	Número aleatorio
M	LMP_sres	Respuesta de autenticación
M	LMP_comb_key	Número aleatorio
M	LMP_unit_key	Llave

Encriptación

Si por lo menos una autenticación se ha realizado se puede utilizar encriptación. Si el maestro quiere que todos los esclavos en la picored utilicen los mismos parámetros de encriptación debe emitir una llave (K_{master}) temporal y hacer de esta llave la llave actual del enlace para todos los esclavos en la picored antes de que comience la encriptación. Esto es necesario si los paquetes broadcast debieran estar encriptados.

Temporización

LMP soporta solicitudes para la precisión de la temporización. Esta información se puede utilizar para minimizar la ventana de escaneo para un tiempo de espera dado y para extender el tiempo máximo de espera. Se puede utilizar también para minimizar la ventana de escaneo cuando se está escaneando por las ranuras del

[31] PIN: por sus siglas en ingles (Personal Identification Number)

modo sniff o los paquetes de aviso del modo park. Los parámetros de precisión de temporización devueltos son la tendencia a largo plazo medidos en ppm y la inestabilidad a largo plazo medida en µs del reloj utilizado durante los modos de hold, sniff y park. Estos parámetros son fijos para cierto dispositivo y deben ser idénticos cuando se solicite varias veces. La precisión de temporización puede ser solicitada en cualquier momento siguiente a un procedimiento exitoso de paginación de banda base. Si no se soporta solicitudes de precisión de temporización, el dispositivo solicitante debe asumir los valores en el peor de los casos (drift=250ppm y jitter=10µs).

Versión y Características

LMP soporta solicitudes para la versión del protocolo LM. El dispositivo solicitado enviará una respuesta con tres parámetros: VersNr, CompId y SubVersNr. VersNr especifica la versión de la especificación Bluetooth LMP que el dispositivo soporta. CompId se usa para rastrear los posibles problemas con las capas Bluetooth más bajas. Todas las compañías que crean una implementación única del Administrador de Enlace tendrán su propio CompId. La misma compañía es también responsable de la administración y mantenimiento del SubVersNr. Para un VersNr y CompId dados, los valores del SubVersNr deben aumentar cada vez que una nueva implementación es lanzada.

El controlador de enlace y radio Bluetooth puede soportar sólo un subconjunto de los tipos de paquetes y características descritas en las Especificaciones de Banda Base y las especificaciones de Radio. Los PDU LMP_features_req[32] y LMP_features_res[33] son utilizados para intercambiar esta información. Las características soportadas se pueden solicitar en cualquier momento siguiente a un procedimiento exitoso de paginación de banda base. Un dispositivo no podrá enviar ningún paquete diferente de ID, FHS, NULL, POLL, DM1 ni DH1 antes de estar enterado de las características soportadas del otro dispositivo. Después que la solicitud de características se ha llevado a cabo, la intersección de los tipos de

[32] LMP_features_req: (Feature requirement – Solicitud de Características)
[33] LMP_features_res: (Feature Response – Respuesta de Características)

paquete soportados para ambos lados se puede transmitir también. Cuando una solicitud es emitida, debe ser compatible con las características soportadas del otro dispositivo.

Cambio del Papel Maestro-Esclavo

Ya que el dispositivo que pagina siempre llega a ser el maestro de la piconet, un cambio del papel maestro-esclavo se necesita a veces.

Si el esclavo inicia el cambio maestro-esclavo, finaliza la transmisión del paquete ACL actual con información L2CAP, detiene la transmisión L2CAP y envía LMP_slot_offset inmediatamente seguido por LMP_switch_req. Si el maestro acepta el cambio maestro-esclavo, finaliza la transmisión del paquete ACL actual con información L2CAP, detiene la transmisión L2CAP y responde con LMP_accepted. Cuándo el cambio se ha completado en el nivel de banda base (exitosamente o no) ambas unidades re-habilitan la transmisión L2CAP. Si el maestro rechaza el cambio responde con LMP_not_accepted y el esclavo re-habilita la transmisión L2CAP. La identificación de la transacción para todos los PDUs en la secuencia es puesta a 1.

Petición de Nombre

LMP soporta la solicitud de nombre a otro dispositivo Bluetooth. El nombre es amigable al usuario asociado con el dispositivo Bluetooth y consiste en un máximo de 248 bytes codificados según el estándar UTF-8. La solicitud de nombre se puede hacer en cualquier momento siguiente a un procedimiento exitoso de paginación de banda base.

Desconexión

La conexión entre dos dispositivos Bluetooth puede ser finalizada en cualquier momento por el maestro o el esclavo. Un parámetro de razón se incluye en el mensaje para informar el otro partido de por qué se finaliza la conexión.

Modo Hold

El enlace ACL de una conexión entre dos dispositivos Bluetooth se puede colocar en modo hold por un tiempo especificado. Durante este tiempo ningún paquete ACL se transmitirá desde el maestro. Se entra al modo hold típicamente cuando no hay la necesidad de enviar datos por un tiempo relativamente largo. El transceptor entonces se puede apagar para ahorrar potencia. Pero el modo hold se puede utilizar también si un dispositivo quiere descubrir o ser descubierto por otros dispositivos Bluetooth, o quiere unirse a otras piconets. Lo que un dispositivo realmente hace durante este tiempo no es controlado por el mensaje hold, pero depende de cada dispositivo decidir.

Modo Sniff

Cuándo el enlace está en el modo sniff el maestro sólo puede comenzar una transmisión en la ranura sniff. Dos parámetros controlan la actividad de escucha en el esclavo. El parámetro de intento de sniff determina por cuántas ranuras el esclavo debe escuchar, comenzando en la ranura sniff, aunque no reciba un paquete con su propia dirección de AM[34]. El parámetro de fin de tiempo de sniff determina por cuántas ranuras adicionales el esclavo debe escuchar si continúa recibiendo sólo paquetes con su propia dirección AM.

Modo Park

Si un esclavo no necesita participar en el canal, pero debería estar sincronizado con los saltos de frecuencia, se puede colocar en modo park. En este modo el dispositivo entrega su AM_ADDR (dirección de miembro activo) pero se re-sincroniza al canal despertando en los instantes de aviso separados por los intervalos de aviso. El intervalo de aviso, un offset de aviso y una bandera indicando cómo el primer instante de aviso se calcula, determina este primer instante. Después de esto los instantes de aviso siguen periódicamente en el intervalo predeterminado. En estos instantes el esclavo parqueado puede ser

[34] AM: (Miembro Activo – Active Member)

activado otra vez por el maestro, el maestro puede cambiar los parámetros del modo park, transmitir información broadcast o permitir a los esclavos parqueados solicitar acceso al canal.

Enlaces SCO

Cuando se ha establecido una conexión entre dos dispositivos Bluetooth, la conexión consiste en un enlace ACL. Unos o más enlaces SCO pueden entonces ser establecidos. El enlace SCO reserva ranuras separadas por el intervalo SCO, Tsco. La primera ranura reservada para el enlace SCO es definida por Tsco y el offset SCO, Dsco. Después de eso las ranuras SCO siguen periódicamente con el intervalo SCO.

Control de Paquetes Multi-Ranura

El número de ranuras utilizadas por un dispositivo se puede limitar. Un dispositivo permite que el dispositivo remoto utilice un número máximo de ranuras enviando el PDU LMP_Max_slot proporcionando ranuras máximas como parámetro. Cada dispositivo puede solicitar el uso de un número máximo de ranuras enviando el PDU LMP_Max_slot_req proporcionando ranuras máximas como parámetro. Dos PDUs se utilizan para el control de paquetes multi-ranura. Estos PDUs pueden ser enviados en cualquier momento después que se complete la configuración de la conexión.

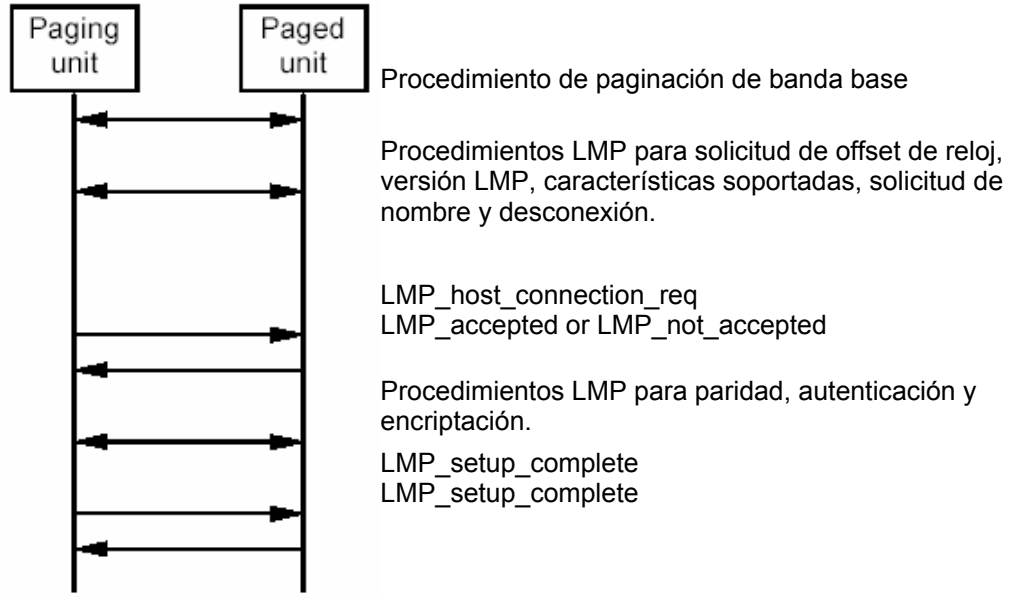
Supervisión de Enlace

Cada enlace Bluetooth tiene un reloj que es utilizado para la supervisión del enlace. Este reloj se usa para detectar la pérdida del enlace causada cuando algún dispositivo se sale del rango, se apaga, u otros casos semejantes. Un procedimiento LMP se utiliza para establecer el valor de tiempo fuera de la supervisión.

3.3.4. Establecimiento de la Conexión

Después del procedimiento de paginación, el maestro debe encuestar al esclavo enviando paquetes de sondeo. El otro lado recibe este mensaje y lo acepta o rechaza, si es aceptado, la comunicación incluyendo las capas superiores se realiza. Procedimientos LMP con solicitud de offset de reloj, versión LMP, características soportadas, solicitud de nombre y desconexión pueden ser llevados a cabo.

Figura 18. Diagrama del establecimiento de la conexión



3.4. PROTOCOLO DE CONTROL Y ADAPTACIÓN DE ENLACE LÓGICO (L2CAP)

El L2CAP (Logical Link Control and Adaptation Layer Protocol) se encuentra sobre el protocolo de banda base y reside en la capa de enlace de datos. Provee servicios de datos orientado a la conexión y no orientado a la conexión a protocolos de capas superiores con capacidad de multiplexación de protocolo, operación de segmentación y reensamblaje, y abstracción de grupos. Permite a

los protocolos y aplicaciones de capa superior transmitir y recibir paquetes de datos L2CAP de hasta 64 kilobytes de longitud.

L2CAP está definido sólo para enlaces ACL. Para cumplir sus funciones, L2CAP espera que la banda base suministre paquetes de datos en full duplex, que realice el chequeo de integridad de los datos y que reenvíe los datos hasta que hayan sido reconocidos satisfactoriamente.

El protocolo de control y adaptación de enlace lógico está basado sobre el concepto de canales. Cada uno de los end-points de un canal L2CAP está asociado a un identificador de canal.

3.4.1. Identificador de Canal

Los identificadores de canal (CIDs – Channel Identifiers) son los nombres locales que representan un end-point de un canal lógico en el dispositivo. Los identificadores desde 0x0001 a 0x003F se reservan para funciones L2CAP específicas. El identificador nulo (0x0000) es definido como un identificador ilegal y nunca se debe utilizar como un end-point de destino.

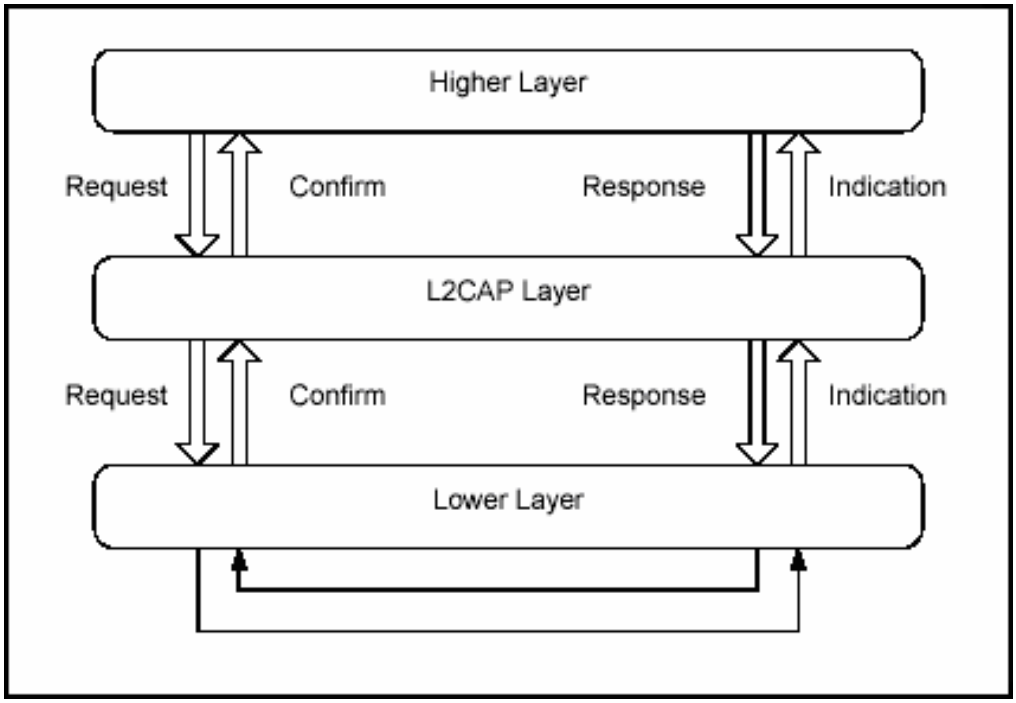
3.4.2. Operación entre Dispositivos

Los canales de datos orientados a la conexión representan una conexión entre dos dispositivos, donde un CID identifica cada end-point del canal. Los canales no orientados a la conexión restringen el flujo de datos a una sola dirección. Hay también varios CIDs reservados para propósitos especiales. El canal de señalización es un ejemplo de un canal reservado. Este canal se utiliza para crear y establecer los canales de datos orientados de la conexión y para negociar cambios en las características de estos canales. El soporte para un canal de señalización dentro de una entidad L2CAP es obligatorio. Otro CID está reservado para todo el tráfico de datos entrante no orientado a la conexión.

3.4.3. Operación entre Canales

Las implementaciones L2CAP deben transportar datos entre protocolos de capas superiores y el protocolo de capa inferior. Cada implementación debe soportar también un conjunto de comandos de señalización para el uso entre implementaciones L2CAP. Las implementaciones L2CAP deben también estar preparadas para aceptar ciertos tipos de eventos desde capas inferiores y generar eventos a capas superiores. Cómo estos eventos se pasan entre capas es un proceso dependiente de la implementación.

Figura 19. Arquitectura L2CAP



3.4.4. Segmentación y Reensamblaje

Las operaciones de Segmentación y Reensamblaje (SAR[35]) se utilizan para mejorar la eficiencia soportando un tamaño de unidad de transmisión máxima (MTU[36]) más grande que el paquete más grande de banda base. Todos los

[35] SAR: por sus siglas en ingles (Segmentation and reassembly)
[36] MTU: por sus siglas en ingles (Maximum Transmission Unit)

paquetes L2CAP se pueden segmentar para la transferencia sobre paquetes de banda base. El protocolo no realiza ninguna operación de segmentación y reensamblaje pero el formato del paquete soporta la adaptación a tamaño físicos más pequeños. Una implementación L2CAP expone el MTU saliente y segmenta paquetes de capa superior en 'pedazos' que pueden pasar al Administrador de Enlace vía la Interfase Controladora de Host (HCI[37]), si existe. En el lado receptor, una implementación L2CAP recibe 'pedazos' desde el HCI y reensambla esos pedazos en paquetes L2CAP utilizando información proporcionada por el HCI y del encabezamiento del paquete.

3.4.5. Eventos

Los eventos son todos los mensajes entrantes a la capa L2CAP junto con timeouts[38]. Los eventos se dividen en cinco categorías: Indicaciones y Confirmaciones desde capas inferiores, Pedidos y Respuestas desde capas superiores, datos desde iguales, Pedidos de señal y Respuestas desde iguales, y eventos causados por expiraciones del reloj.

3.4.6. Acciones

Todos los mensajes y timeouts enviados desde la capa L2CAP son llamados acciones. Las acciones se encuentran divididas en cinco categorías: Confirmaciones e Indicaciones a capas superiores, Pedidos y Respuestas a capas inferiores, Pedidos y Respuestas a Iguales, transmisión de datos a iguales, y configuración de reloj.

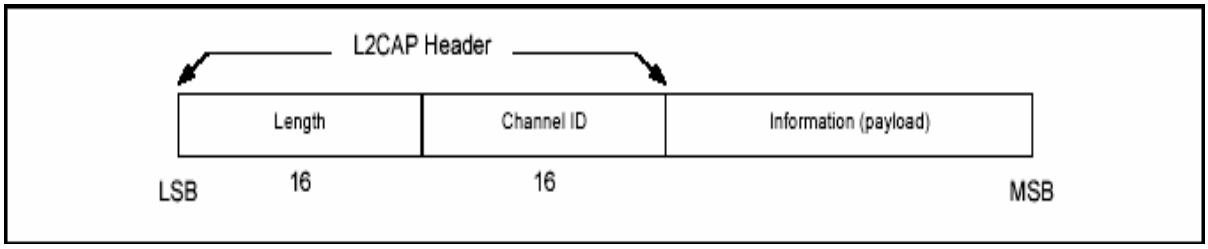
3.4.7. Formato del Paquete de Datos

L2CAP está basado en paquetes pero sigue un modelo de comunicación basado en canales. Un canal representa un flujo de datos entre entidades L2CAP en dispositivos remotos. Los canales pueden ser o no orientados a la conexión.

[37] HCI: por sus siglas en ingles (Host Controller Interface)
[38] Timeouts: tiempo de espera excedido

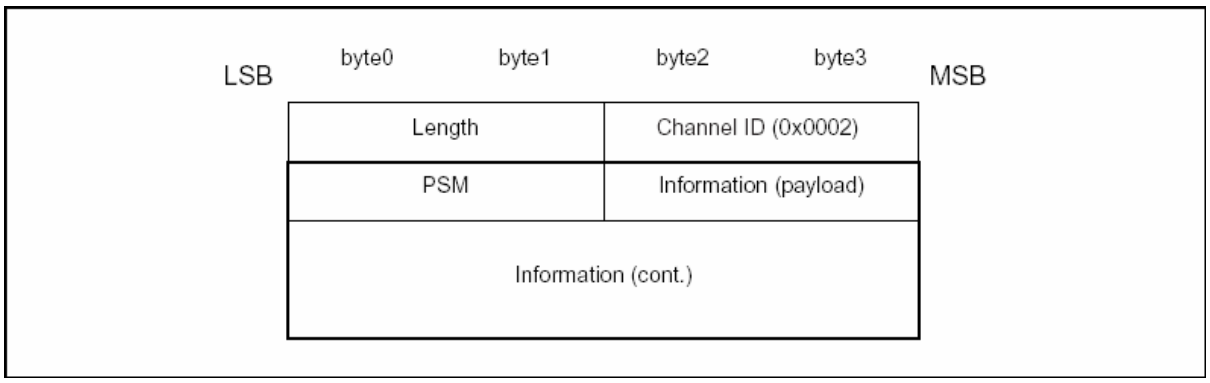
Los paquetes de canal orientado a la conexión están divididos en tres campos: longitud de la información, identificador de canal, e información.

Figura 20. Paquete L2CAP



Los paquetes de canal de datos no orientados a la conexión son iguales a los paquetes orientados a la conexión pero adicionalmente incluyen un campo multiplexor de protocolo y servicio (PSM – Protocol/Service Multiplexer).

Figura 21. Paquete de canal de datos no orientados a la conexión



3.4.8. Opciones de Configuración de Parámetro

Las opciones son un mecanismo para extender la habilidad de negociar diferentes requisitos de conexión. Las opciones son transmitidas en la forma de elementos de información comprendidos por un tipo de opción, una longitud de opción, y uno o más campos de datos de opción.

Unidad Máxima de Transmisión (MTU – Maximum Transmisión Unit)

Esta opción especifica el tamaño de la carga útil que el emisor es capaz de aceptar. Ya que todas las implementaciones L2CAP son capaces de soportar un tamaño mínimo de paquete L2CAP, esto no es realmente un valor negociado sino más bien un parámetro de información para el dispositivo remoto de que el dispositivo local puede acomodar en este canal un MTU más grande que el mínimo requerido. En el caso improbable de que el dispositivo remoto sólo esté dispuesto a enviar paquetes L2CAP en este canal, más grandes que el MTU anunciado por el dispositivo local, entonces este Pedido de Configuración recibirá una respuesta negativa en la que el dispositivo remoto incluirá el valor de MTU que se intenta transmitir. En este caso, su implementación especifica si el dispositivo local continuará el proceso de configuración o mantendrá aún este canal.

Opción de Timeout de vaciado

Esta opción se utiliza para informar al recipiente de la cantidad de tiempo que el controlador de enlace / administrador de enlace del emisor intentará transmitir exitosamente un segmento L2CAP antes de rendirse y evacuar el paquete.

Opción de Calidad de Servicio (QoS – Quality of Service)

Cuándo se incluya en un Pedido de Configuración, esta opción describe el flujo del tráfico saliente del dispositivo que envía el pedido al dispositivo que lo recibe. Cuándo se incluye en una Respuesta de Configuración positiva, esta opción describe el acuerdo del flujo del tráfico entrante visto desde el dispositivo que envía la respuesta. Cuándo se incluye en una Respuesta de Configuración negativa, esta opción describe el flujo del tráfico entrante preferido desde la perspectiva del dispositivo que envía la respuesta.

Las implementaciones L2CAP sólo se requieren para soportar servicio de “Mejor Esfuerzo”; soporte para cualquier otro tipo de servicio es opcional. “Mejor

Esfuerzo" no requiere ninguna garantía. Si ninguna opción de QoS se coloca en el pedido, "Mejor Esfuerzo" se debe asumir. Si cualquier garantía de QoS se requiere entonces un pedido de configuración de QoS debe ser enviado.

Algunos dispositivos pueden requerir un alto rendimiento o una respuesta rápida. Antes de que un dispositivo con grandes peticiones se conecte a una piconet, este trata de obtener una garantía de servicio. En este caso la respuesta incluirá valores específicos como rata de transmisión, tamaño del buffer de tráfico, ancho de banda, tiempo de recuperación de datos, etc. Por lo tanto, antes de que el maestro conecte a un nuevo esclavo o actualice la configuración de calidad, debe chequear si posee timeslots y otros recursos libres.

3.5. PROTOCOLO DE DESCUBRIMIENTO DE SERVICIO (SDP)

El SDP[39] proporciona medios a las aplicaciones cliente para descubrir la existencia de servicios prestados por las aplicaciones servidor y para determinar los atributos de esos servicios. Los atributos de un servicio incluyen el tipo o clase de servicio ofrecido y el mecanismo o información de protocolo necesitada para utilizar el servicio.

3.5.1. Descripción General

SDP implica comunicación entre un servidor SDP y un cliente SDP. El servidor mantiene una lista de registros de servicio que describe las características de servicios asociados con el servidor. Cada registro de servicio contiene información acerca de un solo servicio. Un cliente puede recuperar información de un registro de servicio mantenido por el servidor SDP publicando un pedido SDP.

Si el cliente, o una aplicación asociada con el cliente, decide utilizar un servicio, debe abrir una conexión separada al proveedor de servicio para utilizar el servicio. SDP proporciona un mecanismo para descubrir servicios y sus atributos, pero no proporciona un mecanismo para utilizar esos servicios.

[39] SDP: por sus siglas en ingles (Service Discovery Protocol)

Hay un máximo de un servidor SDP por dispositivo Bluetooth. (Si un dispositivo Bluetooth actúa sólo como un cliente, no necesita servidor SDP). Un solo dispositivo Bluetooth puede funcionar tanto como un servidor SDP o un cliente SDP. Si múltiples aplicaciones en un dispositivo proporcionan servicios, un servidor SDP puede actuar a favor de ésos proveedores de servicios para manejar los pedidos de información acerca de los servicios que ellos proporcionan.

3.5.2. Registro de Servicios

Un servicio es una entidad que puede brindar información, ejecutar una acción o controlar un recurso a nombre de otra entidad. Un servicio puede ser implementado como software, hardware, o una combinación de estos.

Toda la información acerca de un servicio que es mantenido por un servidor SDP se contiene dentro de un solo registro de servicio. El registro de servicio consiste enteramente en una lista de atributos de servicio.

Cada atributo de servicio describe una sola característica de un servicio. Un atributo de servicio se compone de dos componentes: una identificación de atributo y un valor de atributo.

Una identificación de atributo es un entero único de 16 bits que distingue cada atributo de servicio de otros atributos de servicio dentro de un registro de servicio. La identificación de atributo identifica también el significado del valor asociado de atributo.

Una definición de clase de servicio especifica cada una de las identificaciones de atributo para una clase de servicio y asigna un significado al valor de atributo asociado con cada identificación de atributo.

Todos los servicios pertenecientes a una clase de servicio dada asignan el mismo significado a cada identificación de atributo particular.

En el Protocolo de Descubrimiento de Servicio, una identificación de atributo a menudo se representa como un elemento de datos.

El valor de atributo es un campo de longitud variable cuyo significado es determinado por la identificación de atributo asociada consigo y por la clase de servicio del registro de servicio en que el atributo se contiene. En el Protocolo de Descubrimiento de Servicio, un valor de atributo se representa como un elemento de datos.

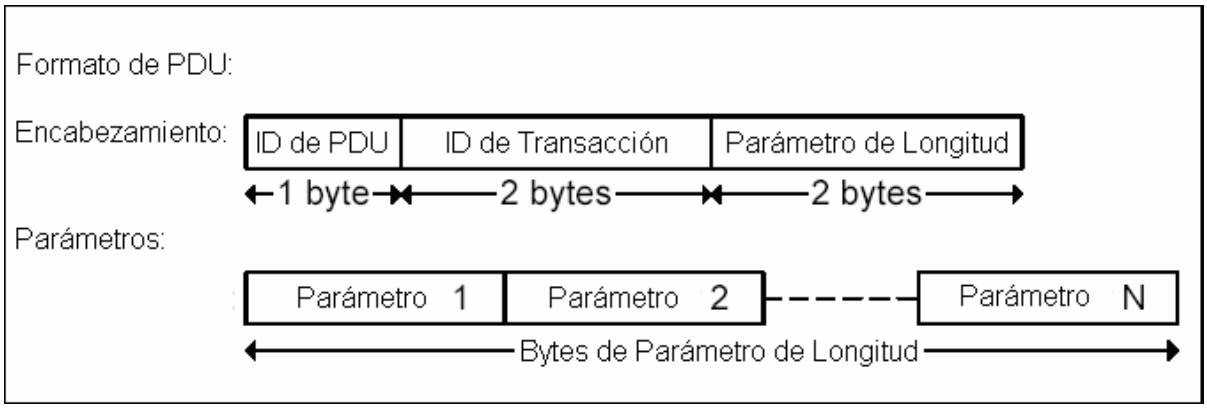
3.5.3. Descripción del Protocolo

SDP utiliza un modelo de pedido/respuesta donde cada transacción se compone de un pedido de unidad de datos de protocolo (PDU[40]) y una respuesta PDU.

El SDP transfiere campos de múltiples bytes en un orden estándar de bytes transfiriendo los bytes más significativos primero.

Cada PDU del SDP se compone de un encabezamiento seguido por parámetros específicos de PDU. El encabezamiento contiene tres campos: una identificación de PDU, una identificación de Transacción, y un Parámetro de longitud.

Figura 22. Formato de PDU



[40] PDU: por sus siglas en ingles (Protocol Data Unit)

Algunos pedidos SDP pueden requerir respuestas que son más grandes de lo que puede caber en una sola respuesta PDU. En este caso, el servidor SDP generará una respuesta parcial junto con un parámetro de estado de continuación. El parámetro de estado de continuación puede ser suministrado por el cliente en un pedido subsiguiente para recuperar la próxima porción de la respuesta completa. El parámetro de estado de continuación es un campo de longitud variable cuyo primer byte contiene el número de bytes de continuación de información adicionales en el campo.

Cada transacción se compone de un PDU de pedido y uno de respuesta. Generalmente, cada tipo de PDU de pedido tiene un tipo correspondiente de PDU de respuesta. Sin embargo, si el servidor determina que un pedido tiene un formato impropio o por cualquier razón el servidor no puede responder con el tipo apropiado de PDU, responderá entonces con un PDU SDP_ErrorResponse.

3.5.4. Transacción de Búsqueda de Servicio

Petición de búsqueda de servicio: se genera por el cliente SDP para localizar registros de servicio que concuerden con el patrón de búsqueda de servicio dado como el primer parámetro del PDU. Al recibir este pedido el servidor SDP examina los registros en su base de datos y responde con una respuesta a búsqueda de servicio.

Respuesta a búsqueda de servicio: se genera por el servidor después de recibir una petición de búsqueda de servicio válida. La respuesta contiene una lista de registros de servicio que maneja, para registros de servicio que concuerden con el patrón de búsqueda de servicio dado en el pedido.

Petición de atributo de servicio: Se genera para recuperar valores de atributo específicos de un registro de servicios específico. Lo que maneja el registro de servicios del registro de servicios deseado y una lista de identificaciones del atributo deseado se suministran como parámetros.

Respuesta a atributo de servicio: El servidor SDP genera una respuesta a una petición de propiedad de servicio válida. Ésta contiene una lista de atributos del registro de servicios requerido.

Petición de búsqueda y atributo de servicio: combina la petición de búsqueda de servicio y la petición de atributo de servicio en una sola petición. Como parámetro, contiene tanto un patrón de búsqueda de servicio como una lista de atributos a ser recuperados desde los registros de servicios que concuerdan el patrón de búsqueda de servicios. La petición y la respuesta son más complejas y pueden requerir más bytes, pero sin embargo, puede reducir el número total de transacciones SDP.

Respuesta de búsqueda y propiedad de servicio: como resultado se puede obtener una lista de atributos del registro de servicios que concuerden con el patrón dado y las propiedades deseadas de estos servicios.

3.6. PROTOCOLO RFCOM

RFCOMM es un protocolo de transporte, con provisiones adicionales para emular los 9 circuitos del Puerto serial RS-232 sobre el protocolo L2CAP.

Este protocolo soporta hasta 60 conexiones simultáneas entre dos dispositivos Bluetooth.

Para propósitos de RFCOM, una vía de comunicación completa involucra dos aplicaciones ejecutándose en dispositivos diferentes con un segmento de comunicación entre ellos.

RFCOMM tiene la intención de cubrir aplicaciones que utilizan los puertos seriales de los dispositivos en los que residen. En la configuración simple, el segmento de comunicación es un enlace Bluetooth de un dispositivo a otro (conexión directa). Si el segmento de comunicación es otra red, se utiliza la tecnología inalámbrica Bluetooth para la vía entre el dispositivo de conexión a la red y un módem. A

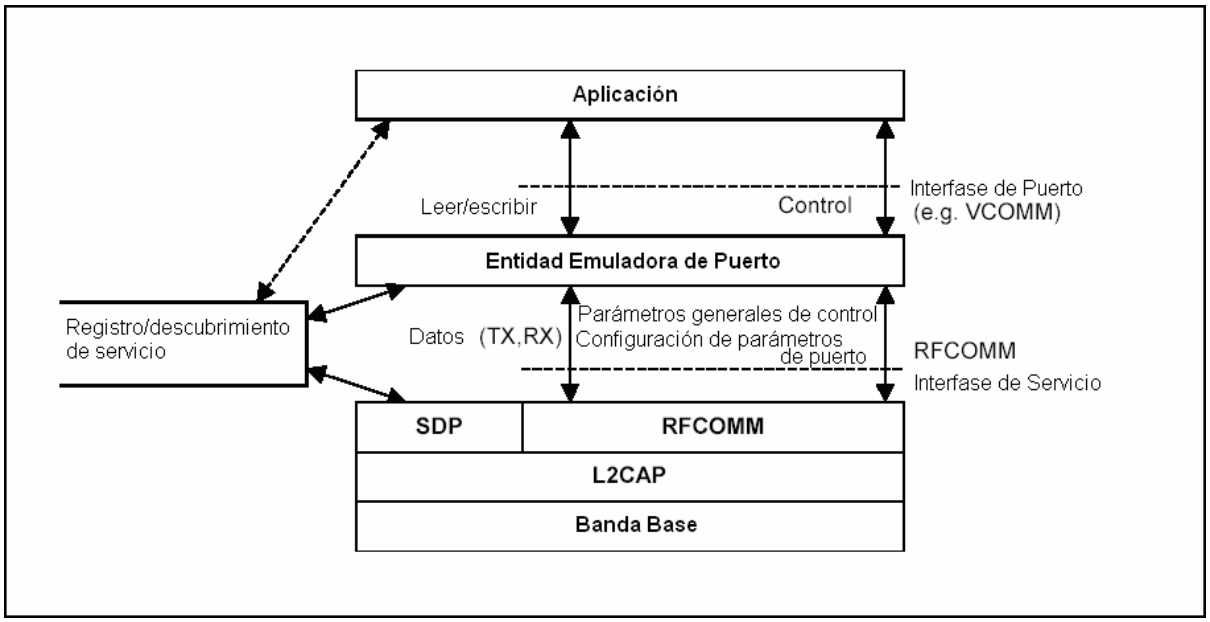
RFCOM solo le concierne la conexión entre los dispositivos en el caso de la conexión directa, o entre el dispositivo y el módem en el caso de la red.

Básicamente dos tipos de dispositivos existen que RFCOM debe acomodar. Dispositivos tipo 1 son puntos finales de comunicación tales como computadoras e impresoras. Dispositivos tipo 2 son aquellos que son parte de un segmento de comunicación como los módems.

El RFCOM está orientado a hacer más flexibles estos dispositivos, soportando fácil adaptación de comunicación Bluetooth. Un ejemplo de una aplicación de comunicación serial es el protocolo punto-a-punto (PPP). El RFCOMM tiene construido un esquema para emulación de null modem y usa a L2CAP para cumplir con el control de flujo requerido por alguna aplicación.

En la mayoría de los sistemas, RFCOM será parte de un driver de puerto que incluye una entidad emuladora de puerto serial. La Figura 23 muestra un modelo de como RFCOM encaja en un sistema típico.

Figura 23. Modelo de RFCOM en un sistema típico



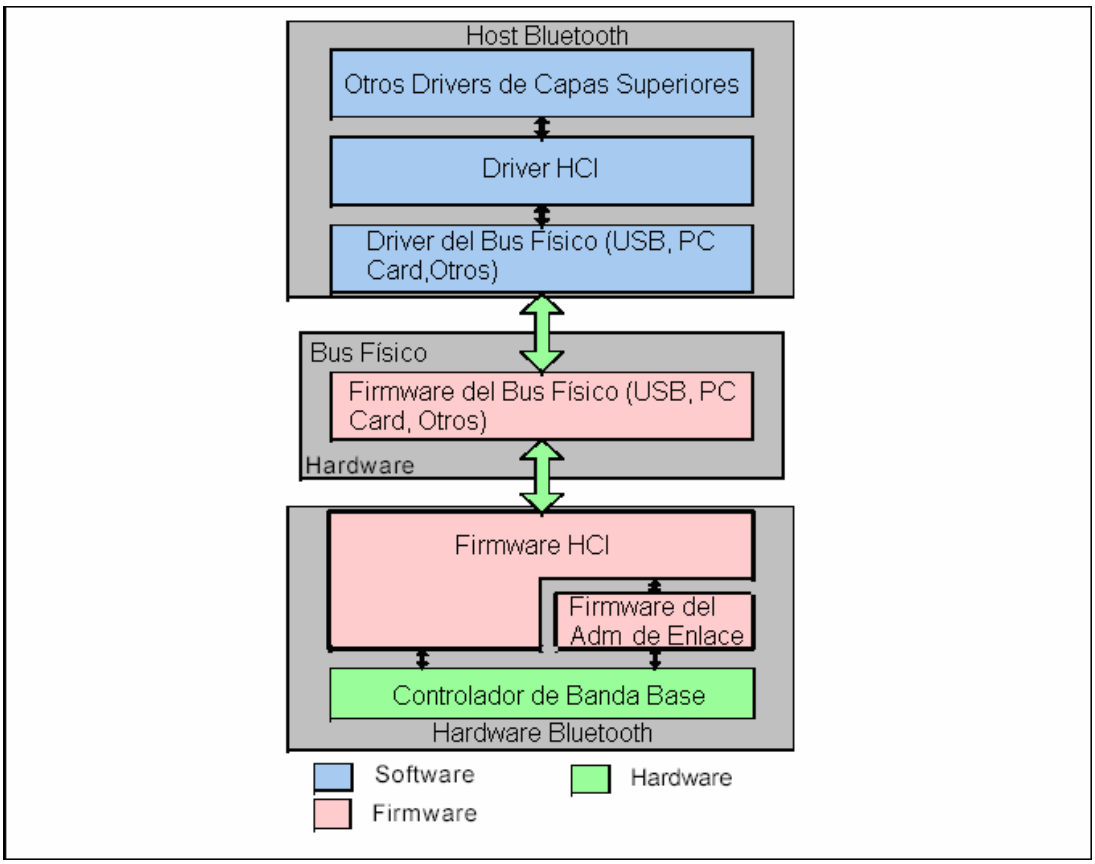
3.7. ESPECIFICACIONES DEL HCI (HOST CONTROLLER INTERFACE)

La HCI (Host Controller Interface) provee un método uniforme de interfase para acceder las capacidades de hardware de Bluetooth.

3.7.1. Capas Inferiores del Stack de Software Bluetooth

La Figura 24 provee una perspectiva de las capas de software inferiores. El firmware HCI implementa los comandos HCI para el hardware Bluetooth accediendo los comandos de banda base, comandos del administrador de enlace, registros de status de hardware, registros de control, y registros de eventos.

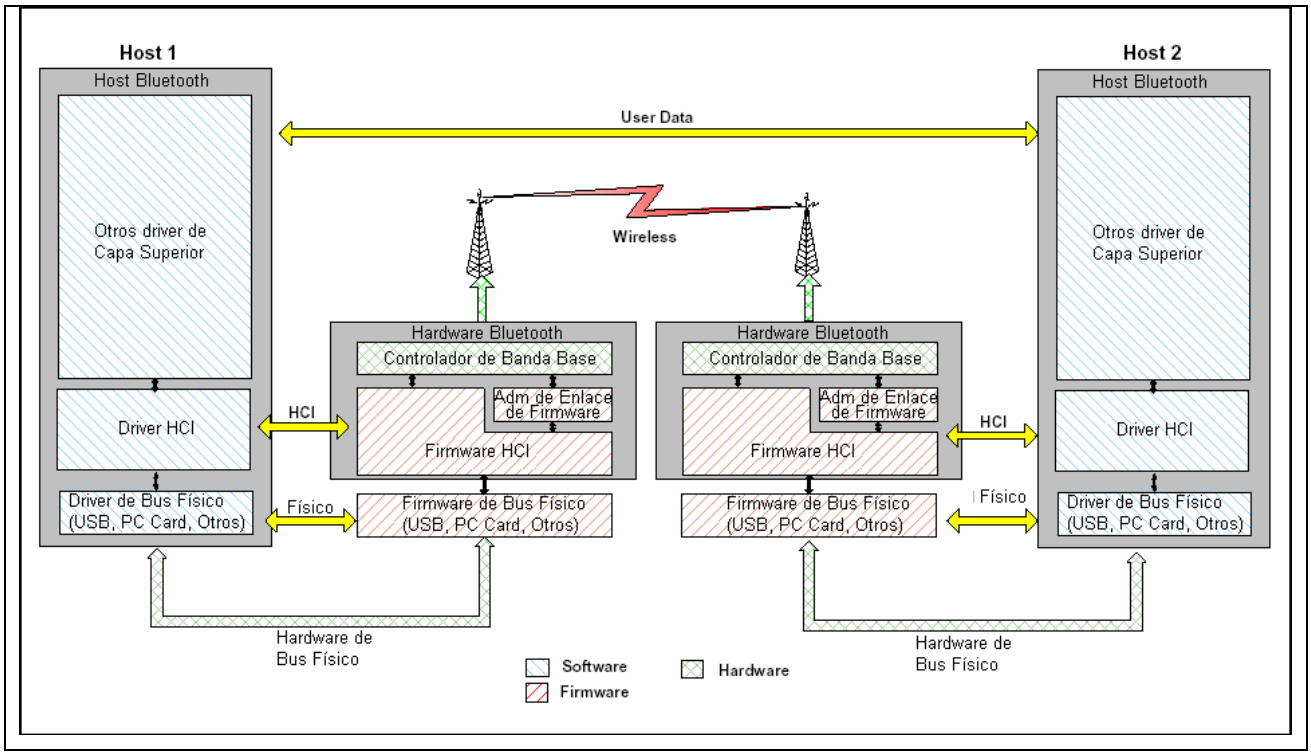
Figura 24. Capas inferiores del stack de software Bluetooth



Varias capas pueden existir entre el driver HCI en el sistema host (huésped) y el firmware HCI en el hardware Bluetooth. Estas capas intermedias, Capa de transporte del Controlador de Host, proveen la habilidad de transferir datos sin conocimiento profundo de estos.

La Figura 25 ilustra la vía de una transferencia de datos de un dispositivo a otro. El driver HCI en el host intercambia datos y comandos con el firmware HCI en el hardware Bluetooth. El driver de la Capa de Transporte de Control de Host provee a ambas capas HCI la habilidad de intercambiar información entre ellas.

Figura 25. Diagrama general end to end de las capas de software más bajas

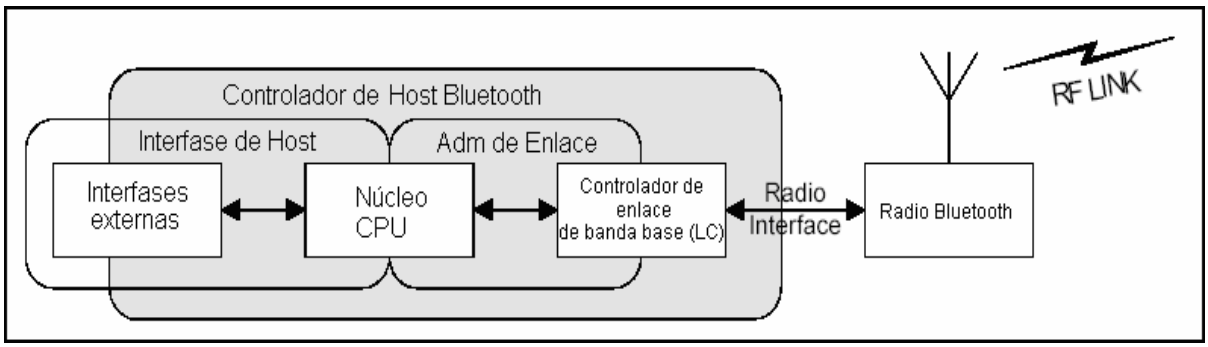


3.7.2. Diagrama de Bloque de Hardware Bluetooth

Una perspectiva general del Hardware Bluetooth se muestra en la Figura 26. Consiste en una parte análoga (la radio Bluetooth) y una parte digital (el Controlador de Host). El controlador de Host tiene un hardware procesador de

señales digitales (Controlador de Enlace – LC – Link Controller), un núcleo de CPU, y hace interfase con el entorno de host.

Figura 26. Diagrama de bloque de hardware Bluetooth



3.7.3. Controlador de Enlace

El Controlador de Enlace (LC – Link Controller) consiste en partes de software y hardware que realizan procesamiento de banda base, y protocolos de capas físicas tales como el protocolo ARQ y codificación FEC.

Las funciones realizadas por el controlador de enlace incluyen:

- Tipos de transferencia con parámetros de Calidad de Servicio (QoS – Quality-of-Service)
- Transferencias asíncronas con entrega garantizada utilizando Petición Rápida de Repetición Automática (fARQ – Fast Automatic Repeat reQuest)
- Transferencias asíncronas
- Codificación de audio
- Encriptación

3.7.4. Núcleo CPU

El núcleo CPU permitirá al módulo Bluetooth manejar Consultas y filtrar peticiones de Paginación sin involucrar al dispositivo host. El Controlador de Host puede ser

programado para responder ciertos mensajes de paginación y autenticar enlaces remotos.

El software Administrador de Enlace (LM[41]) se ejecuta en el núcleo CPU. El LM descubre otros LMs remotos y se comunica con ellos por medio del Protocolo Administrador de Enlace (LMP[42]) para realizar su rol de proveedor de servicio utilizando los servicios del Controlador de Enlace (LC[43]) subyacente.

3.7.5. Posibles Arquitecturas de Bus Físico

Los dispositivos Bluetooth tendrán varias interfases de bus físico que se podrían utilizar para conectar al hardware Bluetooth. Estos buses pueden tener arquitecturas y parámetros diferentes.

Arquitectura de la HCI de USB

USB puede manejar varios canales lógicos sobre el mismo canal físico (por medio de Puntos Finales). Por lo tanto el control, los datos, y los canales de la voz no requieren ninguna interfaz física adicional.

Arquitectura de la HCI de la PC Card

A diferencia del USB, todo tráfico entre el Host y el módulo Bluetooth irá a través de la interfase de bus de la PC Card. Comunicaciones entre el PC del host y el módulo Bluetooth se harán principalmente directamente a través de registros/memorias.

La pila del driver del host tiene una capa de transporte entre el driver Controlador de Host y el Controlador de Host. El objetivo principal de esta capa de transporte es la transparencia. Al driver Controlador de Host (que le habla al Controlador de Host) no debe importarle si está ejecutándose sobre USB o PC Card. Tampoco

[41] LM: por sus siglas en ingles (Link Manager)
[42] LMP: por sus siglas en ingles (Link Manager Protocol)
[43] LC: por sus sigas en ingles (Link Controller)

deben requerir el USB o la PC Card ninguna visibilidad hacia los datos que el driver Controlador de Host pasa al Controlador de Host.

Los comandos de enlace de la HCI proveen al Host la habilidad de controlar las conexiones de la capa de enlace a otros dispositivos Bluetooth. Estos comandos típicamente involucran al Administrador de Enlace (LM) para intercambiar comandos del LMP con dispositivos Bluetooth remotos.

4. APLICACIONES INDUSTRIALES

Las plantas industriales se componen de muchos dispositivos interconectados de maneras diferentes. Quizás sean las unidades (E/S) sencillas para la recolección de datos sin alguna inteligencia incorporada, dispositivos más inteligentes (por ejemplo sensores con inteligencia incorporada, controladores de un solo lazo o controladores programables) y sistemas de supervisión (usados como HMI: Human Machine Interface). Estos tipos de dispositivos se interconectan usando muchos protocolos diferentes de comunicación y medios, que pueden en algunos casos ser reemplazados con la tecnología inalámbrica Bluetooth.

4.1. REDES INALAMBRICAS.

Bluetooth es un protocolo de comunicaciones inalámbrico de corto alcance y bajo consumo de potencia en la banda ICM de 2,4 GHz que soporta tanto tráfico de datos como de audio. Su enlace es tan altamente confiable que hace de la tecnología una de las más aptas para cualquier tipo de aplicación en comunicaciones digitales, ya que habilita mecanismos de detección de error, ofrece una inmunidad natural a la interferencia empleando espectro disperso de salto de frecuencia FHSS a 1600 saltos por segundo y habilita procesos de encriptación para garantizar comunicaciones confiables y seguras.

Todos los dispositivos que formen una red Bluetooth conmutan al unísono bajo el control de uno de ellos (maestro).

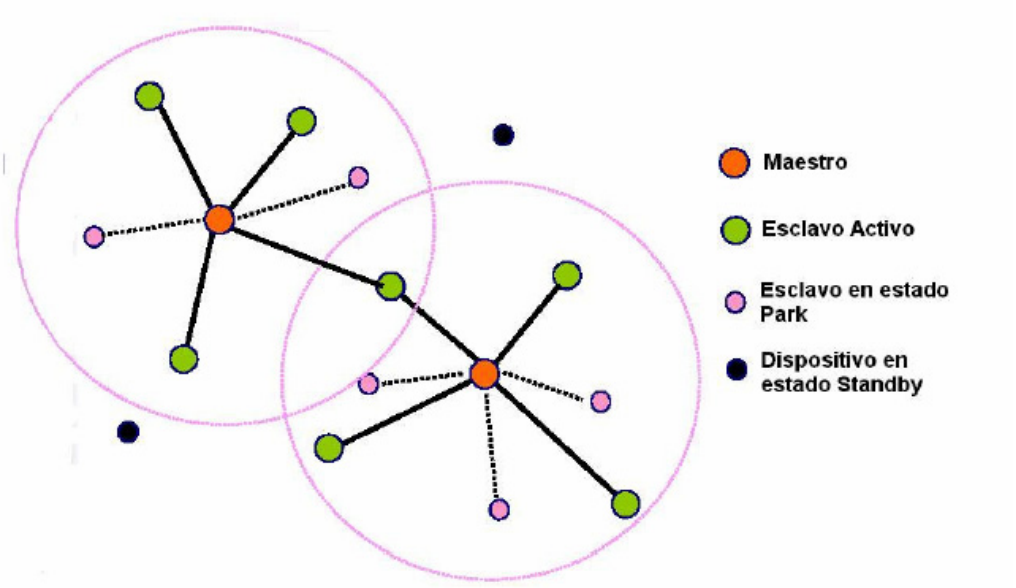
Cada canal Bluetooth es capaz de soportar tres canales full-duplex para ser utilizados, por ejemplo, en transmisión de voz (64 Kb/seg) o un canal full-duplex y

otro half-duplex, por ejemplo, para transmitir datos. En este caso el canal half-duplex podría transmitir 721 Kb/seg en un sentido y 56 Kb/seg en el otro, o tal vez 432,6 Kb/Seg en ambos sentidos.

Una red Bluetooth (también llamada piconet) debe estar formada siempre por un maestro (que envía la información de reloj para la sincronización, mas la información de salto de frecuencia) y hasta siete esclavos (slaves).

Las piconets pueden conectarse entre ellas, formando una scatternet, cuando dos dispositivos que pertenecen a piconets diferentes, se conectan.

Figura 27. Ejemplo de una scatternet



En ambientes industriales es común el monitoreo de muchos parámetros eléctricos o mecánicos donde Bluetooth puede formar una red de sensores e instrumentos de medida removiendo las conexiones físicas entre estos y un centro de captura de datos. También permitiría la conexión, monitoreo y programación de controladores lógicos programables PLC's, RTU's, y puntos de campo instalados en líneas o plantas de producción.

En los laboratorios, la utilización de Bluetooth está dada por la capacidad de conectar en red instrumentos y equipos programables por puertos serial o USB. En los hogares y oficinas, la tecnología muestra unos de sus más claros ejemplos al eliminar los cables para la conexión en red de PC's, con monitores, teclados, ratones, impresoras, scanners y otros periféricos como PDA's y teléfonos celulares.

4.2. INTERNET

Una mayor inteligencia interna en los dispositivos proporciona al usuario un producto más preparado y bien probado. Esto le da al fabricante del dispositivo la posibilidad de "empacar" el conocimiento de su dominio sin revelar los secretos del negocio. También hace más eficiente el mantenimiento y la resolución de problemas. EL dispositivo podría almacenar localmente información importante que da al ingeniero de mantenimiento los medios para realizar un trabajo más eficiente. La interfaz de usuario (UI – User-Interface) interna basada en Internet podría visualizar el status del dispositivo desde puntos de vista de diferentes categorías. Bluetooth se suma a la facilidad de uso, primero proveyendo medios para acceder de manera muy sencilla la interfase de usuario del dispositivo y segundo proporcionando la habilidad de leer y escribir datos. Combinando Bluetooth y la interfaz de usuario basada en tecnología Internet, un usuario podría utilizar el dispositivo portátil con la Interfaz Humano Máquina (HMI – Human-Machine-Interface) que normalmente carga consigo para acceder la UI del dispositivo.

La HMI del dispositivo inteligente es expuesta al usuario utilizando la tecnología de Internet, por ejemplo la World Wide Web (WWW) y/o las interfaces WAP. La idea básica es que la UI integrada pueda ser utilizada en cualquier tipo de dispositivo HMI estándar. El único requisito es que un navegador estándar HTML (o WAP) esté disponible en el dispositivo HMI y que Bluetooth sea soportado como un medio para la comunicación basada en IP. El aspecto positivo acerca de esto es que todos los dispositivos portátiles incluirán esto en un futuro cercano lo que nos

permitirá utilizar teléfonos móviles, PDAs y laptops como HMI hacia dispositivos industriales.

La idea es incluir páginas Web en el dispositivo para usuarios de diferentes categorías como por ejemplo, para el personal de mantenimiento, páginas de ayuda en caso de mantenimiento y localización de errores. Los operadores podrían utilizar la HMI para supervisar el dispositivo, para las personas configurando el sistema existen páginas que brindan ayuda.

4.3. BUSES DE CAMPO

Actualmente la mayoría de aplicaciones industriales implican el uso de una gran cantidad de elementos de campo como sensores y actuadores. Dados los requerimientos actuales de la integración dentro de un entorno totalmente automatizado, estos elementos de campo no solo deben ser capaces de realizar complicadas funciones sino que también deben ser capaces de comunicarse y trabajar en conjunto con otros equipos, de acuerdo a las necesidades finales del usuario. Los equipos por tanto, en principio, deben tener la conformidad de un estándar de comunicación. Estos dispositivos tienen que satisfacer primeramente las pruebas de conformidad del estándar de comunicaciones que implementarán, pero muchas veces esto no es un requisito suficiente para poder trabajar en conjunto porque entre implementaciones que tienen la conformidad de un estándar puede que sea imposible el funcionamiento conjunto. Por consiguiente, deben también ofrecer otras propiedades como las llamadas interoperabilidad o cooperación entre dispositivos. Cuando tratamos temas relativos a la integración de dispositivos de campo, es necesario en primer lugar poder distinguir claramente los siguientes conceptos: conformidad, interconectividad, interoperabilidad, cooperación e intercambiabilidad.

Los medios de transmisión son los elementos por los que se transporta la información, haciendo que llegue con la menor cantidad de ruido y distorsión a todos los nodos (o estaciones) involucrados en el proceso de comunicación. A

nivel de campo deben permitir mucha flexibilidad en cuanto a manejo físico del mismo y al incremento del número de nodos de manera simple.

De manera ineludible, asociado a los medios de transmisión se encuentran los conectores que permiten realizar la unión entre los nodos y elementos de la red y el medio de transmisión, debiendo ser transparentes al funcionamiento de la misma, sin entorpecer o atenuar el flujo de señales.

Dependiendo del tipo de red a instalar, a menudo estos conectores suelen ser específicos, aunque existen conectores de uso general como los conectores DB9, DB15 y DB25 habitualmente empleados en transmisión de señales eléctricas.

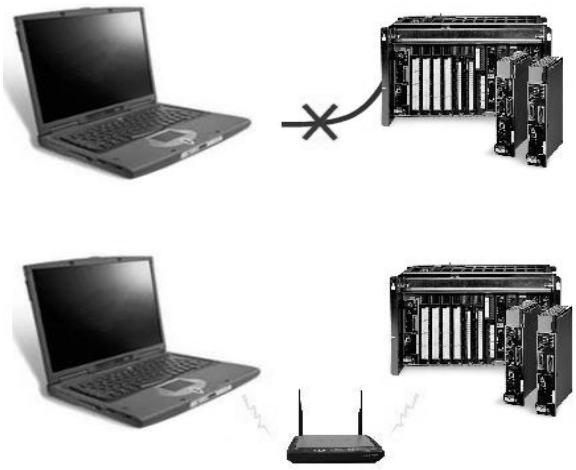
Existen dos clases principales de medios de transmisión, los medios guiados, y los medios no guiados. En el primer tipo existe un medio material por donde se transmite la información (cableado en general), y el segundo tipo utiliza el aire como medio de transmisión, es decir, suelen ser sistemas de transmisión inalámbricos. La elección de un tipo de red local conlleva la elección del medio de transmisión pues cada fabricante suele recomendar un tipo de medio de transmisión que mejor se adapta a la red, o bien aconseja varios medios de transmisión dependiendo de las distancias, velocidades de transmisión, ancho de banda, entorno de trabajo, etc.

En emplazamientos donde resulta complicado trazar un tendido de cable, es conveniente utilizar un enlace inalámbrico. Actualmente, este tipo de enlaces está teniendo un gran auge debido a la aparición de sistemas de enlace como Wi-Fi (IEEE 802.11b) y Bluetooth, que resuelven las comunicaciones entre dispositivos en distancias cercanas, pero donde se centran gran parte de las necesidades de los usuarios (por ejemplo, en una nave industrial). Sin embargo, los enlaces mediante medios no guiados ya se vienen realizando con anterioridad mediante ondas de radio para distancias cercanas, y mediante enlaces de microondas, usados generalmente en enlaces punto a punto que deben cubrir largas distancias (se usan para comunicaciones terrestres y vía satélite).

4.4. REEMPLAZO DE CABLE SERIAL

Muchos dispositivos industriales de hoy usan la interface tradicional serial como medio para conectar herramientas de configuración o herramientas de programación (interfaces como RS232, RS422 o RS485). Estas son típicas conexiones cuando una reconfiguración o reprogramación se necesitan y normalmente operar en un PC normal. Las herramientas usan típicamente una aplicación dependiente o el dispositivo de protocolo específico de comunicación para comunicar con el dispositivo. Todo esto los hace un candidato bueno para una conexión de Bluetooth. El ejemplo en la figura 28 muestra una PC base programadora conectado a un PLC (Controlador Programable de Lógico) usando un cable serial.

Figura 28. Reemplazo de Cable Serial



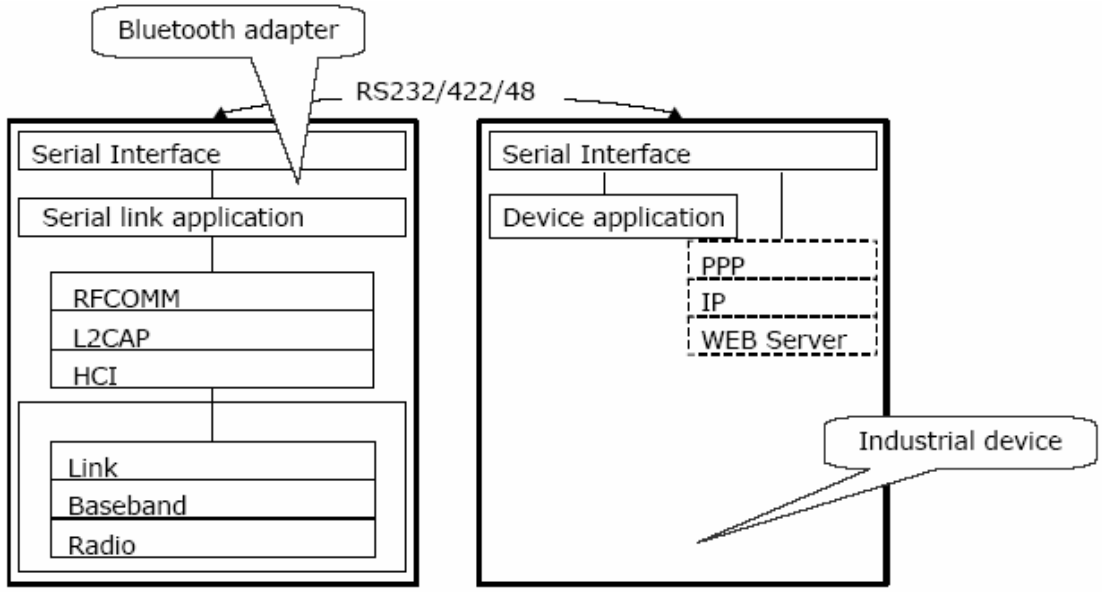
Hay dos maneras de hacer un reemplazo de cable serial. O usar un adaptador externo de Bluetooth conectado a un puerto externo serial del dispositivo industrial o un adaptador incorporado conectado internamente a la electrónica actual del dispositivo. El adaptador de Bluetooth emula un puerto serial y usa el protocolo RFCOMM para transferir los datos sobre el aire (es soportado por el Perfil del Puerto Serial). El PC tiene incorporado Bluetooth, la Tarjeta del PC o usa otro componente adicional. La implementación del PC Bluetooth expone el Bluetooth el

Perfil del Puerto Serial como un COMMport emulado, permite la configuración ya existente de PC y las herramientas de programación para ser usadas.

Otra opción del reemplazo del cable está disponible para dispositivos industriales más avanzados, los dispositivos que soportan TCP/IP y un servidor WEB. En este caso el adaptador de Bluetooth sostiene el Perfil del Acceso LAN hasta el nivel RFCOMM y el resto del montón de software se incluye en el dispositivo industrial (PPP, IP y el servidor WEB). Esto permite HMI (Interface Hombre Maquina) dispositivos externos (por ejemplo PC Portátiles o PDAs) eso sostiene el Perfil del Acceso LAN, para conseguir acceso a la WEB se incorpora un dispositivo con una interface al usuario. Ninguna de las aplicaciones específicas del software necesitan ser instaladas en el dispositivo HMI.

La Figura 29 muestra la arquitectura básica del adaptador Bluetooth para el reemplazo del cable serial.

Figura 29. Arquitectura Básica Adaptador Bluetooth Reemplazo de Cable Serial.



4.5. COMBINACIÓN DE BLUETOOTH E INTERNET

Asuma una válvula con un sistema incorporado del control normalmente expone sus variables dinámicas de la posición y el control por un protocolo estándar Modbus (Figura 30).

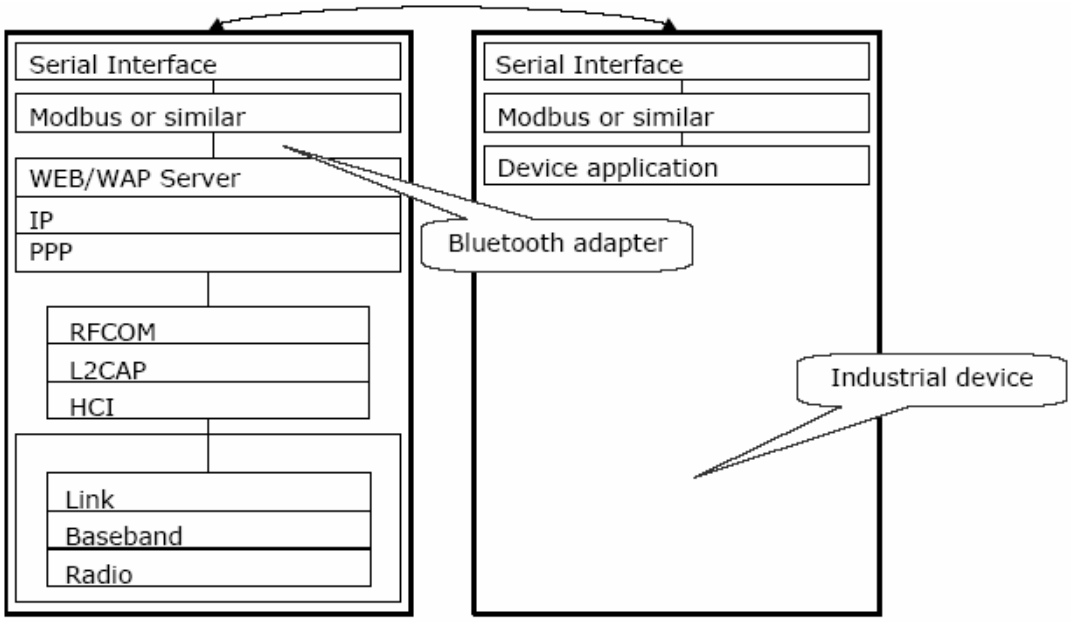
Figura 30. Protocolo estándar Modbus

Un adaptador de Bluetooth es conectado al dispositivo (externo o incorporado). El adaptador de Bluetooth comunica a la válvula que usa el protocolo Modbus. La pagina WEB/WAP conseguida por un acceso al servidor WEB/WAP solía demostrar y modificar los datos dinámicos que se leen y escriben por el protocolo Modbus. Las paginas WEB/WAP son accesibles por Bluetooth usando el Perfil del Acceso LAN. Use esto en páginas WEB para configurar, mantener y supervisar el dispositivo.

La arquitectura de este concepto se describe en la Figura 31.

Como indicada en la figura, otros protocolos industriales que Modbus quizás se use como protocolo de comunicación entre el sistema del control del dispositivo y el adaptador de Bluetooth.

Figura 31. Arquitectura Básica Adaptador Bluetooth Comunicación Modbus.



Use Wap sobre el teléfono móvil de Bluetooth para conseguir acceso a un usuario incorporado con interface WAP. El WAP sobre la especificación de Bluetooth incluye la funcionalidad de un "direccionamiento" incluida como parte de la funcionalidad del teléfono. Esto permite que una página local WAP incluya un hyperlink a otra página localizada en algún lugar en la Red de Área Extensa (WAN). La WAN puede tener acceso usando GMS, GPRS o las tecnologías futuras de UMTS. Un escenario típico es un demostrar una alarma con la pagina local WAP. La página contiene un enlace a una página WAN con una información detallada que contiene acerca de cómo resolver el problema indicado por la alarma. La página WAN se puede actualizar constantemente con la información más reciente con respecto a la alarma.

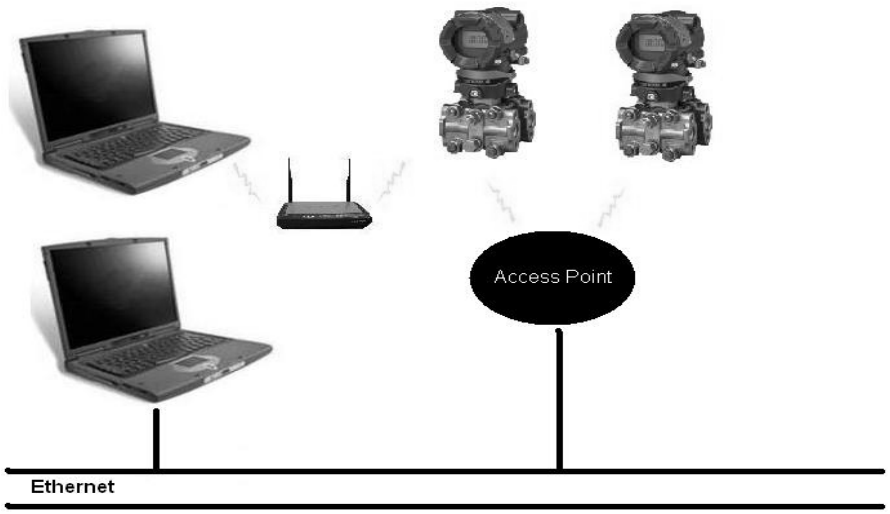
4.6. PUNTOS DE ACCESO INDUSTRIAL

El uso de comunicación inalámbrica en un ambiente industrial será un proceso gradual. Esto nos requiere crear las islas inalámbricas de Bluetooth habilitadas para los dispositivos conectados a una existente red alambrada. La red alambrada

puede ser una red basada el estándar IP (por ejemplo Ethernet) o una red industrial de fieldbus (por ejemplo Profibus, Devicenet, Controlnet o Interbus).

El primer ejemplo es una red alambrada basada en Ethernet y una isla de dispositivos industriales habilitados con Bluetooth (ver Figura 32). Los dispositivos industriales (en este caso válvulas) usan servidores WEB ensamblados sobre Bluetooth.

Figura 32. Combinación Ethernet – Bluetooth.



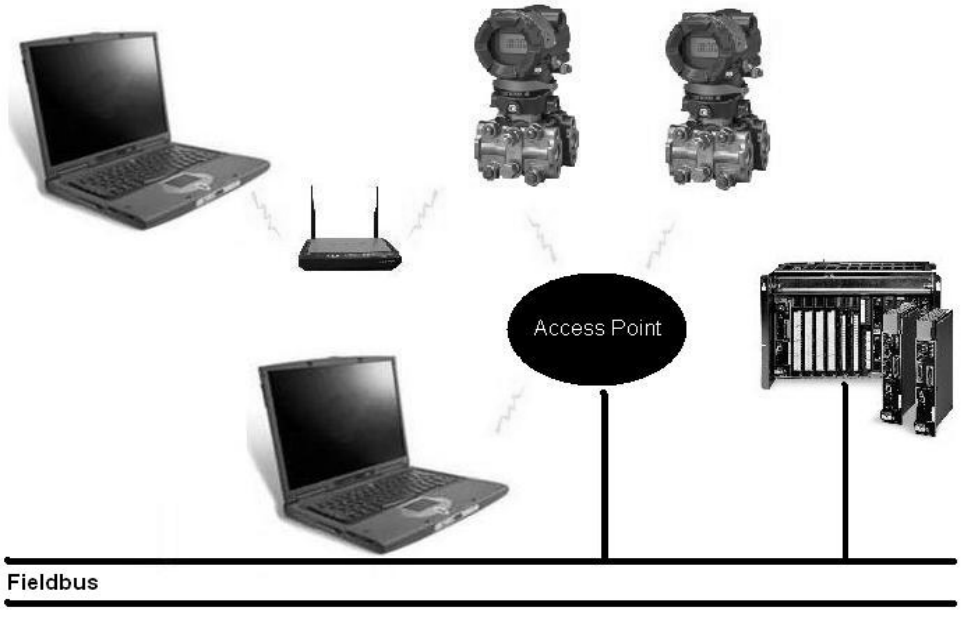
El dispositivo con interfase WEB consigue el acceso al Punto de Acceso (AP). El AP actúa como un “cambio de teléfono” conecta a las válvulas individuales. Un usuario de la WEB “navega” en el AP. Usar una interfase WEB incorporada en el AP hace una lista de todos los dispositivos conectados de Bluetooth se demuestra. El usuario escoge un dispositivo y una conexión del Perfil del Acceso LAN es establecida al dispositivo y los comienzos de AP actuando como un router. Al mismo tiempo los dispositivos individuales basados en WEB la HMI hace un acceso directo de Bluetooth.

El segundo ejemplo es una variante del ejemplo arriba. El Punto de Acceso (AP) actúa como un AP que llama usando un MODEM, GSM, GPRS o las tecnologías futuras de UMTS (ve la Figura 33).

Figura 33. Combinación Telefonía Móvil – Bluetooth.

Hay una variación grande de fieldbuses disponible en la industria de hoy, ambos estándar y el vendedor específico. Los ejemplos siguientes muestran dispositivos habilitados con Bluetooth (válvulas en el ejemplo) conectado a un existente red alambrada que usa un “Punto de Acceso Fieldbus” (ve la Figura 34).

Figura 34. Combinación Fieldbus – Bluetooth.



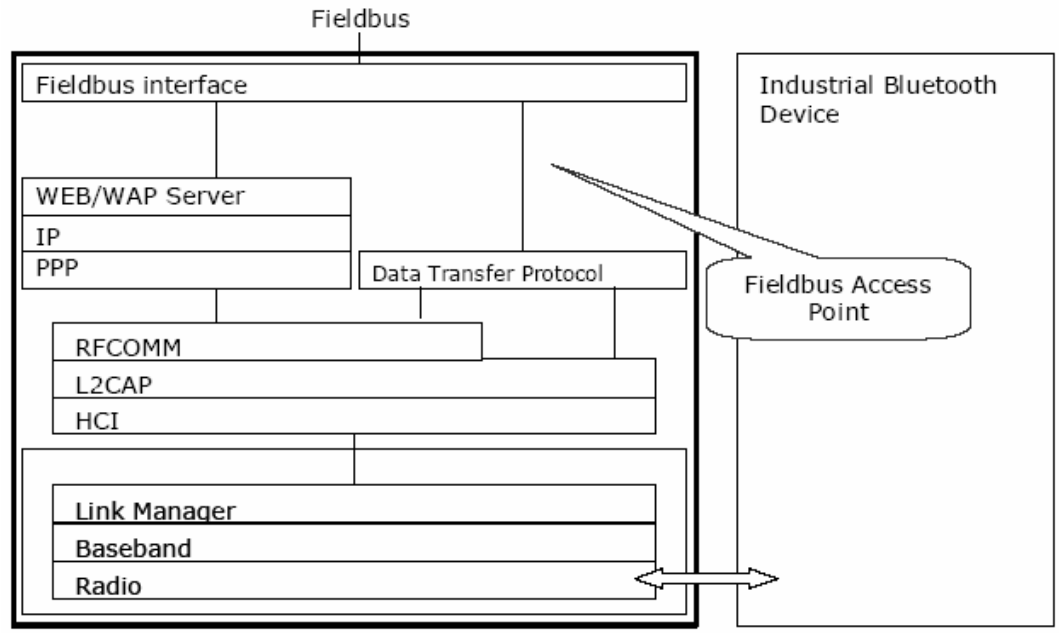
En este escenario los datos son transferido del dispositivo Bluetooth al usar el punto de acceso a datos específicos “protocolo de transferencia” encima de Bluetooth. Los datos son “convertidos” al formato soportado por el fieldbus y transferidos a un dispositivo que solicita conexión a algún lugar en la red fieldbus.

Como indicado en la figura, el dispositivo Bluetooth se puede usar simultáneamente como un dispositivo de Internet con un HMI basado en WEB incorporado (ve la sección previa) y como un dispositivo para transferir y colección de datos del punto de acceso (y adicional al fieldbus).

Otra opción deberá soportar el Perfil del Acceso LAN de Bluetooth y a un servidor WEB incorporado en el Punto de Acceso. Esto conseguirá acceso a los datos recuperados de los dispositivos de Bluetooth y de dispositivos conectados al fieldbus que usa un HMI basado en WEB.

La Figura 35 muestra la arquitectura básica de un “Punto de Acceso Fieldbus”.

Figura 35. Arquitectura Básica Adaptador Bluetooth Comunicación Fieldbus.



El protocolo de transmisión de datos es un protocolo específico del dominio que opera encima de la pila del protocolo Bluetooth. Puede llamar la pila de Bluetooth en el nivel L2CAP o el nivel de RFCOMM. El mismo protocolo se debe soportar en la implementación de Bluetooth del dispositivo industrial. Esto es un área donde la interoperabilidad entre dispositivos de diferentes fabricantes es un deseo y quizás es uno de las tareas para un futuro Grupo de Trabajo Industrial dentro del SIG

4.7. REDES DE SENSORES

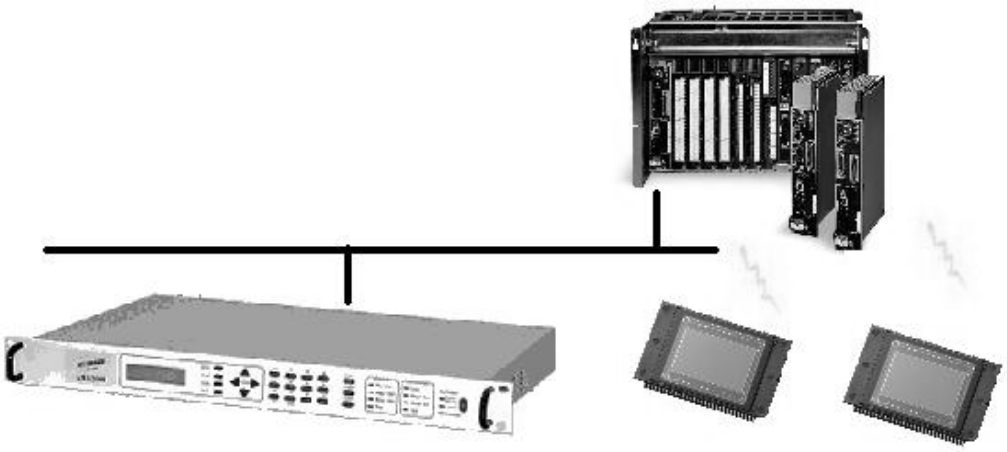
Los sensores y actuadores pueden ser de diferentes tipos. Algunos sensores y actuadores tienen un alto nivel de inteligencia integrada, otros son sólo simples dispositivos de entrada y salida sirviendo de interfases finales al equipo de proceso. Dependiendo de esto, los requisitos en una solución inalámbrica Bluetooth pueden diferir. Un dispositivo inteligente puede incluir funcionalidad local lo suficientemente buena para mantener el proceso andando en un modo limitado si se pierde la conexión. Esto se puede hacer dividiendo el algoritmo de control en dos partes, una para el control de supervisión, ejecutándose en un sistema huésped y una para el control crítico de la misión, ejecutándose localmente en el sensor/actuador. Esto podría también ser una solución cuando el criterio de rendimiento es mayor que lo disponible en Bluetooth. Lazos de control rápidos y recolección rápida de datos se ejecutan sobre bluetooth y los datos almacenados en un búfer son transmitidos utilizando Bluetooth.

Diferentes tipos de procesos también tienen diferentes requerimientos en la solución Bluetooth. Algunos procesos imponen demandas limitadas en rendimiento y podrían estar hoy en día muy bien equipados para control en tiempo real utilizando Bluetooth.

Los sensores inalámbricos y actuadores están muy bien equipados para aplicaciones en equipos industriales móviles. Un buen ejemplo son los sensores de vibración situados en ejes móviles. Esto implica una necesidad de soluciones de energía alternativas para poder soportar una completa solución inalámbrica.

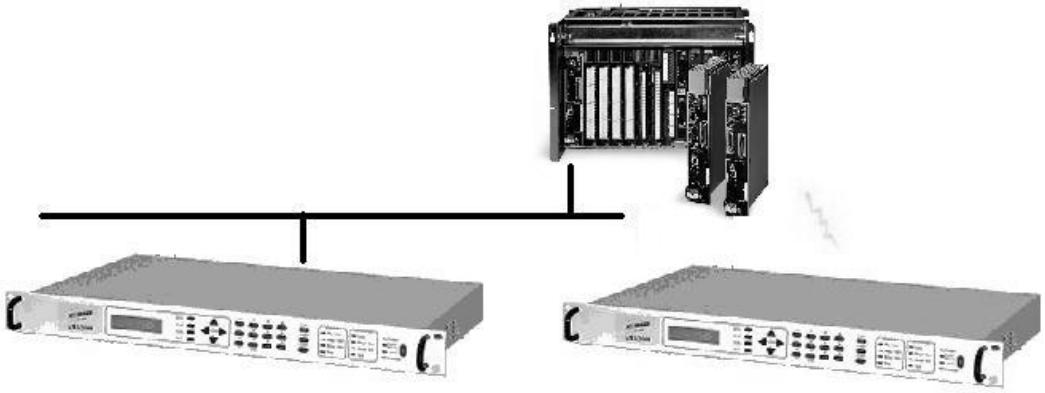
Bluetooth con su soporte para modos de baja potencia se ajusta muy bien a esto, pero los requerimientos necesitan atención especial cuando se desarrolla una solución.

Figura 36. Combinación PLC – Bluetooth.



El primer ejemplo (ver la Figura 36) muestra un sistema de control (PLC) con algunos dispositivos de entrada/salida conectados a través de un bus cableado estándar de entrada/salida y dos sensores/actuadores más inteligentes (en este caso controladores de lazo único). Los controladores de lazo único podrían seguir operando si la conexión Bluetooth es interrumpida temporalmente.

Figura 37. Sistema de Control utilizando Bluetooth



El segundo ejemplo (ver Figura 37) muestra un sistema de control con algunos de los dispositivos simples de entrada/salida conectados utilizando Bluetooth. Este escenario requiere una atención especial para poder asegurar una comunicación segura. Por ejemplo, utilizar esta solución en un proceso donde los requisitos de tiempo real sean bajos de manera que permita retransmisiones si una interferencia temporal perturba el enlace o que opere en un ambiente controlado donde el patrón de interferencia sea conocido.

5. EL FUTURO DE BLUETOOTH

La tecnología Bluetooth abre nuevas posibilidades para el uso de comunicaciones inalámbricas en entornos industriales debido a su bajo precio y seguridad incorporada. La comunicación inalámbrica tiene, sin embargo, ventajas y desventajas inherentes que se deben considerar cuidadosamente cuando se utilice la tecnología inalámbrica en un entorno industrial.

Las principales ventajas de la comunicación inalámbrica son:

- No hay necesidad de cables de comunicación
- Topología flexible
- Son posible un mayor número de aplicaciones

Las principales desventajas son:

- Sensible a interferencias (comparte radio-frecuencias con otros dispositivos)
- Seguridad (confidencialidad, integridad, manipulación de mensajes, privacidad)
- Resistencia y detección de negación de servicio (interferencia)

Para poderse beneficiar de las ventajas más obvias, que son movilidad y remoción de todos los cables, se tiene que resolver el problema de la fuente de poder. Muchas aplicaciones quieren una eliminación completa de cables por lo que la potencia se debe obtener por medios como baterías, generación local, paneles solares, etc.

Bluetooth tiene diferentes ventajas y desventajas comparada con las tecnologías inalámbricas en general. Las principales ventajas de Bluetooth son:

- Bajo costo, baja potencia
- Seguridad, que está integrada

Las principales desventajas son:

- Ancho de banda compartido con muchos otros sistemas
- Rango corto, grandes retrasos
- Sensible a interferencias

Los enlaces Bluetooth estarán disponibles en todas partes, y permitirán que los equipos industriales operen entre sí con computadores portátiles, palm tops, y teléfonos móviles. El bajo costo de esta tecnología también permite su introducción en otras aplicaciones como sensores, recolección de datos, monitoreo, etc.

5.1. REQUISITOS INDUSTRIALES DE BLUETOOTH

Bluetooth se diseñó originalmente para la comunicación entre equipos de computadores, teléfonos móviles y periféricos. Puede ser utilizado como punto de acceso de voz y datos, reemplazo de cables, etc. Los paquetes son optimizados para aplicaciones de voz, transferencia de datos, y aplicaciones como tarjetas de negocios, números de teléfonos, etc. Las aplicaciones industriales son de alguna forma diferentes. Los mensajes son por lo general cortos, pero es importante que la información se transfiera rápidamente y de manera segura. La graduación de tiempo de esos mensajes también es ampliamente utilizada. Bluetooth tiene actualmente un esquema ARQ (excepto para los paquetes de voz), que hace que una transferencia determinística de datos sea muy difícil. En las futuras versiones de Bluetooth, la transferencia transparente de paquetes deberá estar disponible. Esto permitirá que las aplicaciones reciban los paquetes en tiempos programados

incluso si estos poseen errores. La aplicación entonces puede decidir si el paquete debe ser retransmitido o si se de debe tomar otra acción.

Los equipos industriales son, a menudo, instalados en entornos difíciles, con temperaturas extremas, vibraciones, etc. Esto requiere que el hardware del módulo Bluetooth utilizado en la industria deba resistir temperaturas desde los -40 hasta los 80 grados Celsius, y que tengan un diseño robusto.

El consumo de potencia es también un gran problema ya que por lo general esta no está disponible. Una batería no es una solución muy atractiva ya que el beneficio de introducir tecnología inalámbrica es opacado por la necesidad de reemplazar baterías regularmente.

Para resumir, los principales requisitos de la industria para Bluetooth son:

- Fiabilidad
- Paquetes de datos transparentes
- Consumo de poder
- Un mayor rango de temperatura

Las redes de sensores inalámbricas se volverán omnipresentes en la industria ya que permiten una forma fácil y económica de mejorar el rendimiento y la productividad. Sistemas inalámbricos altamente confiables y seguros con inteligencia distribuida permitirán a la industria explotar poderosas posibilidades que ofrecen los nuevos sensores y ejercer de manera confiable un control más cercano de procesos críticos de producción.

5.2. METAS DEFINIDAS POR LA INDUSTRIA

Para lograr su visión del futuro, la comunidad industrial de sensores inalámbricos necesitará alcanzar una serie de metas y objetivos de rendimiento. Para poder alcanzar estas metas, se requiere avances claves en potencia, confiabilidad, integración, costo, funcionalidad, y eficiencia en el ancho de banda.

5.2.1. Potencia

A través de mejoras en el diseño, los sistemas inalámbricos de sensores del futuro requerirán un menor consumo de potencia y por lo tanto menos mantenimiento que los sistemas actuales. Dentro de algunos años, los costos asociados con la operación y mantenimiento de estos sistemas disminuirán en un 90 por ciento. A largo plazo, los sistemas serán auto-energizados, capturando la energía del entorno industrial (energía solar, energía vibratoria) y eliminando virtualmente las actividades de mantenimiento de potencia y su respectivo costo.

Los sistemas inalámbricos utilizarán inteligencia incorporada para procesar datos de sensores y minimizar el consumo de potencia. Estos sistemas de sensores inteligentes utilizarán un sistema de reporte que minimice las transmisiones para reducir, simultáneamente, el consumo de potencia y la interferencia.

5.2.2. Confiabilidad / Mantenibilidad / Disponibilidad

Los sistemas inalámbricos del futuro realizarán de manera confiable misiones críticas de monitoreo y funciones de control. Los requerimientos de mantenimiento para estos sistemas serán mínimos, ya sea reemplazo de baterías, verificación de la calibración de sensores, o cualquier otra actividad necesaria para mantener el rendimiento del sistema. El tiempo medio entre atenciones del sistema inalámbrico será por lo menos igual a los periodos programados de mantenimiento de otros equipos de producción por lo que el sistema inalámbrico no perturbará la producción o causará su interrupción.

Los sistemas inalámbricos y sus componentes serán construidos para soportar las temperaturas extremas, vibraciones, y otros ambientes severos típicos de operaciones industriales. Además serán inmunes a generadores cercanos de radio frecuencias e interferencia de trayectoria múltiple de señales reflejadas.

La confiabilidad del rendimiento de los sistemas futuros será lo suficientemente alta para que se pueda depender de ellos para realizar funciones esenciales.

5.2.3. Integración / Compatibilidad

Los sistemas inalámbricos del futuro operaran con una arquitectura de infraestructura abierta sin propietario que facilitará el procesamiento y transmisión de datos hacia y desde sensores y controladores producidos por diferentes compañías. Los sistemas serán capaces de manejar salidas de sensores de todo tipo, incluyendo los nuevos y los que ya estén puestos. A corto plazo, estos sistemas deberán proveer interoperabilidad en el nivel de datos. A largo plazo, deberán proveer interoperabilidad en el nivel de conocimientos, de manera que el sistema pueda analizar y actuar con la información.

5.2.4. Costo

A lo largo de la siguiente década, los avances tecnológicos y drivers económicos pondrán a los sensores inalámbricos en la vía de crecimiento en rendimiento de manera constante y descenso de costos.

Las presiones competitivas continúan forzando a los usuarios industriales a buscar nuevas estrategias para modernizar sus operaciones. Los sensores inalámbricos integrados representan una herramienta prometedora ya que su costo continúa descendiendo. A corto plazo, el costo de instalación de un sistema inalámbrico deberá ser de una décima parte del costo de instalación actual. A largo plazo, muchos sensores serán componentes integrales del equipo de producción, y su costo estará incorporado en el costo del equipo.

5.2.5. Funcionalidad

Los componentes de los sistemas inalámbricos del futuro deberán ser capaces de reconocerse mutuamente y organizarse de manera automática para llevar a cabo comunicaciones efectivas, eficientes y seguras. Estos dispositivos de computación

inteligentes, distribuidos, heterogéneos deberán ser casi auto-sostenibles. Las exigencias del usuario serán mínimas a medida que el sistema se vuelva auto-configurable, auto-calibrado, auto-identificable, y auto-reorganizado para un rendimiento de la red y recuperación de fallas óptimos.

La función de seguridad es un asunto significativo en un número cada vez mayor de aplicaciones industriales. La seguridad e integridad de la red debe ser protegida contra la curiosidad y los ataques. Los niveles de protección deben ser escalables y fijados de acuerdo a las posibles ramificaciones de acceso.

La seguridad se puede fortalecer utilizando tecnologías avanzadas de modulación, codificación, encripción, e inter-estratificación.

Las metas de seguridad se pueden expresar en términos del tiempo requerido para lograr el acceso no autorizado. La seguridad es un blanco constante, y los sistemas inalámbricos del futuro deben ser extensibles para permanecer en la delantera de los avances en herramientas y técnicas para lograr el acceso.

5.2.6. Eficiencia de Ancho de Banda

El crecimiento de la tecnología inalámbrica industrial dará a lugar una gran demanda del estrecho ancho de banda disponible actualmente. El uso eficiente del ancho de banda es imperativo para reducir la interferencia y evitar el crecimiento resultante en el uso de potencia. Los desarrolladores de sistemas necesitarán incluir una estrategia para la conservación del ancho de banda para evitar requerimientos de potencia mayores y sus costos asociados. Utilizarán inteligencia alojada para reducir las cargas de transmisión cuando sea posible y utilizar la cantidad mínima de potencia para mantener una comunicación efectiva.

6. CONCLUSIONES

En la industria actual es parte integral de todo proyecto la interconexión de los equipos que hacen parte de un proceso; al llevar a cabo la ingeniería pertinente es de vital importancia poner gran atención al cableado, esto incluye no solo los cables en sí en los cuales hay que considerar aspectos básicos como el calibre, la longitud, su capacidad y parámetros de seguridad, además la forma de transportar estos cables a través de la planta para lo que se tiene en cuenta los diámetro de las tuberías si es por aire junto con su soportería y espacio requerido y si es subterráneo la cuestión se complica más teniendo que tener en cuenta todo lo anterior además de la excavación.

La tecnología inalámbrica elimina todos estos problemas facilitando la interconexión de los equipos y su intervención que cualquier prueba o configuración en campo se puede realizar utilizando un simple PDA, LapTop o cualquier otro dispositivo capaz de tener un acceso al lenguaje de la Internet.

Bluetooth con sus altas cualidades de seguridad y su tecnología de salto de frecuencia es capaz de evitar las interferencias de una manera simple y rápida, además por la alta frecuencia a la que trabaja es capaz de evitar objetos facilitando así el diseño de las plantas.

Existen muchas clases de procesos con diferentes prioridades y requerimientos de velocidad, partiendo de estos hechos es factible diseñar en la actualidad mediante la interconexión de diferentes tecnologías el uso de conexiones tanto alambradas como inalámbricas lo cuál podría reducir los costo y el espacio utilizado.

Las grandes ventajas para la utilización de la tecnología Bluetooth, son el tamaño reducido y el bajo consumo de potencia, esto le da la capacidad de utilizarse en cualquier lugar, en la colocación de equipos terminales, sin estorbar a otros instrumentos.

Hay que determinar que a los inicios de esta tecnología, era un poco costosa, por ser tan innovadora y eficiente. A la vez que en el mercado ya se encuentra muchos fabricantes de esta tecnología, ya que la competencia en el mercado hace que esta reduzca los precios considerablemente, con relación al comienzo de la tecnología Bluetooth. Esto hace que esta misma se mejore en cuanto a calidad y cobertura dentro de la misma.

Una importante aspecto a considerar al momento de determinar el uso de la tecnología inalámbrica, es el mantenimiento que se le debe hacer a los cables cuando estos se encuentra en condiciones extremas de corrosión, creando muchas perdidas en la transmisión, lo cuál se debe realizar constantemente en estos lugares. Con la tecnología inalámbrica todo esto se acaba, solamente se fabrican equipos un poco mas resistentes para este tipo de condiciones otorgando una mayor confiabilidad y reduciendo así los requerimientos de mantenimiento.

Es importante notar la necesidad de mejoras en la tecnología Bluetooth en los aspectos de confiabilidad en la transmisión debido a que existen procesos que no soportan retransmisiones, y con la constante tendencia a la eficiencia de los procesos, es muy cercano el momento en que todos serán así para lo cuál se debe preparar y así explotar sus más grandes atributos de facilidad, economía y ahorro de espacio.

GLOSARIO

ACL: asynchronous Connectionless (asíncrono no orientado a la conexión).

ANSI: American National Standards Institute.

API: application program interface (Interfaz del programa de aplicación).

ARQUITECUTURA: intel, ARM (iPaq, ARM9 y otras) y PowerPC (iMac) entre otras.

ATM: (modo de transferencia asíncrona) dentro del medio informático hace referencia a la conmutación de paquetes (cells -- celdas o células) de un tamaño fijo con alta carga, rápida velocidad (entre 1,544 Mbps. y 1,2 Gbps) y una asignación dinámica de ancho de banda. También se conoce como "paquete veloz" (fast packet).

BD_ADDR: dirección del dispositivo Bluetooth.

BNEP: Bluetooth network encapsulation protocol.

BQP Bluetooth Qualification Program.

CAD: computer aided design (diseño asistido por computador).

CID: identificador de canal.

CRC: chequeo de redundancia cíclica.

DBI: sigla para “decibeles relativos a una fuente isotrópica”.

DCE: data communications equipment. Dispositivo que provee una trayectoria de comunicación entre dos equipos. Por ejemplo el módem en un computador.

DRIVER: controlador que permite gestionar los periféricos que están conectados al ordenador (http://www.guiahost.com/servicios/glosario).

ETHERNET: red de área local (LAN) desarrollada por Xerox, Digital e Intel. Es el método de acceso LAN que más se utiliza (seguido por Token Ring). Ethernet es una LAN de medios compartidos. Todos los mensajes se diseminan a todos los nodos en el segmento de red (http://www.guiahost.com/servicios/glosario).

ETSI: European Telecommunications Standards Institute. Organización sin ánimo de lucro cuya misión es crear estándares de telecomunicaciones para ser usados por décadas en Europa (http://www.etsi.org).

FCC: Comisión Federal de Comunicaciones. Su principal función es la de mantener el control sobre el amplio sector de las telecomunicaciones en los Estados Unidos (http://www.guiahost.com/servicios/glosario).

FIFO: first In first out. El primero en entrar es el primero en salir.

FIRMWARE: parte del software de un ordenador que no puede modificarse por encontrarse en la ROM o memoria de sólo lectura, Read Only Memory. Es una mezcla o híbrido entre el hardware y el software, es decir tiene parte física y una parte de programación consistente en programas internos implementados en memorias no volátiles. Un ejemplo típico de Firmware lo constituye la BIOS. (http://www.guiahost.com/servicios/glosario).

GAP: generic access profile (perfil genérico de acceso).

GNU: es un acrónimo recursivo para ``no es Unix'' Se crea en 1984 sin mucho éxito, bajo la filosofía del software libre, muy al estilo de UNIX.

GOEP: generic object exchange profile (perfil genérico de intercambio de objetos).

GPL: licencia pública general (general public license), desarrollada por la FSF o Free Software Foundation. Puede ser instalado sin limitación en uno o varios ordenadores. En las distribuciones de estos programas debe estar incluido el código fuente.

HARDWARE: componentes electrónicos y electro-mecánicos de una computadora o cualquier otro sistema. Este término es usado para distinguir estos componentes físicos de los datos y programas.

HCI: host controller interface (interfaz controladora del host).

HEC: chequeo de redundancia cíclica de encabezados.

HOST: sistema microprocesado programable (PCs, teléfonos celulares, mouse, impresoras, teclados, sensores inalámbricos, etc.), capaz de ejecutar las líneas de código correspondientes al stack de protocolos Bluetooth para el host.

HW / FW: hardware / firmware.

I2C: interfaz de datos de dos líneas (SDA y SCL) que utiliza palabras de 8 bits y es usada para comunicar memorias, controladores de video, preamplificadores de audio y otros dipositivos.

IAC: codigo de acceso de búsqueda.

IFA: inverted F antenna (antena en F invertida).

ISM: industrial, scientific, medical**.**

L2CAP: logical link controller and adaptation protocol (protocolo de adaptación y control de enlace lógico).

LMP: link manager protocol (Protocolo del administrador de enlace).

ME: management entity (entidad de administración o manejo).

MODULO BLUETOOTH: módulo multichip que implementa en hardware y firmware las capas bajas del stack de protocolos Bluetooth.

MTU: maximun transmission unit.

PAD: punto de conexión del terminal de un dispositivo.

PAGING: servicio para transferencia de señalización o información en un sentido, mediante paquetes, tonos, etc…

PAN: personal area networking.

PATH: es la trayectoria de una pista en un circuito impreso.

PCB: printed Circuit Board (Tarjeta de circuito impreso).

PPP: point to point protocol (Protocolo punto-a-punto).

QoS: calidad de servicio.

RF: radio frecuencia.

RFCOMM: serial port emulation basado en el estándar ETSI TS07.10.

SAR: segmentación y reensamblado.

SCO: synchronous connection oriented (Síncrono orientado a la conexión).

SDAP: service discovery aplication protocol (perfil de aplicación de descubrimiento de servicio).

SDP: service discovery protocol (protocolo de descubrimiento de servicio).

SIG: special interest group.

SOCKET: es una abstracción de red para los terminales de un canal. El Socket está asociado con el protocolo; usualmente, el PF_INET es usado para asociar un socket con el protocolo TCP/IP.

TIMEOUT: tiempo de espera excedido.

TIMESLOT: ranura de tiempo. En Bluetooth tiene una duración de 625 us.

TRANSCEIVER: transmisor-receptor.

UART: el transmisor receptor universal asíncrono (universal asynchronous receiver transmitter), es un dispositivo que multiplexa datos paralelos en seriales para ser transmitidos y convierte en paralelos los datos seriales recibidos.

WAP: wireless application protocol (protocolo para aplicaciones inalámbricas).

REFERENCIAS

- Industrial use of Buetooth, Matts Andersson, CTO
- Disponible en Internet http://www.connectblue.se
- Bluetooth wireless Technology specifications. Version 1.1.
- Bluetooth Connect without cables, BRAY Jennifer y STURMAN Charles
- Disponible en Internet http://www.bluetooth.org
- Implementación del protocolo Bluetooth para la conexión inalámbrica de dispositivos electrónicos programables, Ricardo Linares y Jimmy Quijano
- Bluetooth Tecnology, www.rfi.de
- Discovering Bluetooth, Michael Millar