

REDES PAN BASADAS EN BLUETOOTH

FRANCISCO JAVIER MOLINA FERNÁNDEZ DE CASTRO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2003

REDES PAN BASADAS EN BLUETOOTH

FRANCISCO JAVIER MOLINA FERNÁNDEZ DE CASTRO

Monografía presentada para optar al título de Ingeniero de Sistemas

Director

GONZALO GARZÓN

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2003

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Cartagena de Indias, 1º de diciembre del 2003

Señores

COMITÉ DE EVALUACIÓN DE PROYECTOS DE GRADO

Facultad de Ingeniería de Sistemas – CUTB

Ciudad

Cordial Saludo:

A través de la presente me permito hacer entrega de la monografía titulada **“REDES PAN BASADAS EN BLUETOOTH”** para su estudio y evaluación, la cual fue realizada por el estudiante FRANCISCO JAVIER MOLINA, de la cual acepto ser su director.

En espera que éste se cumpla con las normas pertinentes establecidas por la institución me despido.

Atentamente,

GONZALO GARZÓN

Ingeniero de Sistemas

Cartagena de Indias, 1º de diciembre del 2003

Señores

COMITÉ DE EVALUACIÓN DE PROYECTOS DE GRADO

Facultad de Ingeniería de Sistemas – CUTB

Ciudad

Cordial Saludo:

A través de la presente me permito hacer entrega de la monografía titulada **“REDES PAN BASADAS EN BLUETOOTH”** para su estudio y evaluación, como requisito fundamental para obtener el título de Ingeniero de Sistemas.

En espera que éste se cumpla con las normas pertinentes establecidas por la institución me despido.

Atentamente,

FRANCISCO JAVIER MOLINA

Código: 0205354

AUTORIZACIÓN

Cartagena de Indias, D.T.C.H.

Yo, **Francisco Javier Molina Fernández de Castro**, identificado con número de cédula 73.577.355 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi Monografía y publicarla en el catálogo online de la Biblioteca.

FRANCISCO JAVIER MOLINA

CONTENIDO

	Página
INTRODUCCION	11
1. RED DE ÁREA PERSONAL (PAN)	13
1.1 CONCEPTO	13
1.2 ESQUEMA DE CONECTIVIDAD DE DISPOSITIVOS	15
2. TECNOLOGÍA BLUETOOTH	16
2.1 NACIMIENTO	16
2.2 ESPECIFICACIONES DE LA TECNOLOGÍA	19
2.2.1 Enlace de Radio	20
2.2.2 Banda Base	21
2.2.2.1 Canal Físico	23
2.2.2.2 Enlace Físico	24
2.2.2.3 Paquetes	25
2.2.2.3.1 Código de Acceso	26
2.2.2.3.2 Encabezado	28
2.2.2.3.3 Tipos de Paquetes	30
2.2.2.3.4 Campo Contenido	31
2.2.2.4 Corrección de Errores	32
2.2.2.5 Canales Lógicos	33
2.2.2.6 Rutinas de Transmisión y Recepción	34

	Página
2.2.2.7 Canal de Control	35
2.2.2.7.1 Definición maestro-esclavo	35
2.2.2.7.2 Estados del controlador de enlace	36
2.2.2.7.3 Establecimiento de la conexión	37
2.2.2.7.4 Modos de conexión	39
2.2.2.8 Direccionamiento de los Dispositivos	40
2.2.2.9 Seguridad	42
2.2.3 Protocolo de Administración de Enlace (Link Manager Protocol, LMP)	44
2.2.3.1 Formato LMP	45
2.2.3.2 Procedimientos LMP	47
2.2.4 Control Lógico de Enlace y Protocolo de Adaptación	48
2.2.4.1 Operaciones Generales	48
2.2.5 Protocolo de descubrimiento del servicio SDP	51
2.2.5.1 Descripción	51
2.2.5.2 Formato de PDU	52
2.2.5.3 Respuestas parciales y estado de la continuación	53
2.2.5.4 Manejo de errores	54
2.2.5.5 Servicios SDP	54
2.2.5.5.1 Registro del servicio	54
2.2.5.5.2 Atributos del Servicio	55
2.2.5.5.3 Clase de servicio	55

	Página
2.2.5.5.4 Descubrimiento del servicio	56
2.2.6 Interfaz controladora de host (HCI)	56
2.2.6.1 Componentes principales HCI	56
2.2.6.2 Comandos HCI	58
2.2.6.3 Eventos HCI, Códigos de Error y Control de Flujo	60
2.2.7 Protocolo de reemplazamiento de cables RFCOMM	61
2.2.7.1 Tipos de dispositivos	61
2.2.7.2 Emulación de múltiples puertos seriales	61
2.2.8 Protocolo de Control de Telefonía Binario	62
2.2.9 Protocolos Adoptados	63
2.2.9.1 PPP	63
2.2.9.2 TCP/UDP/IP	64
2.2.9.3 Protocolo OBEX	64
2.2.9.3.1 Formato de contenidos	65
2.2.9.4 WAP	66
3. IMPLEMENTACION	67
4. APLICACIONES	68
CONCLUSIONES	70
GLOSARIO	72
BIBLIOGRAFIA	74

LISTAS DE TABLAS

Tabla1. Clases de código de acceso	Página 27
Tabla 2. Tipos de paquete	30
Tabla3. Modos de conexión Bluetooth	40
Tabla 4. Modos de seguridad	43
Tabla 5. Procedimientos LMP	47
Tabla 6. Comandos HCI	59

INTRODUCCIÓN

En los últimos años, en el mundo de las tecnologías de información, la expansión que ha tenido el intercambio de información a través de la telefonía móvil, ha servido de base para que aquellas personas y empresas que trabajan en el mundo de las redes saquen provecho las ventajas que representa este tipo de comunicación al no tener que depender de cables para la transmisión de datos. Esto último es lo que ha hecho de las redes basadas en dispositivos inalámbricos ganen terreno frente a las redes cableadas.

Dentro de las redes inalámbricas encontramos un tipo muy especial, que está tomando un gran auge gracias a los beneficios de automatización que representan para usuarios que trabajan con ellas. Esta red es conocida como WPAN (Red inalámbrica de área personal), la cual está basada en una tecnología de punta denominada Bluetooth cuyo funcionamiento es a través de las ondas de radio de corto alcance y que día a día está teniendo mayor difusión a nivel mundial.

Una WPAN basada en Bluetooth tiene como finalidad, ser una red de bajo costo que permita conectar equipos informáticos y de comunicación portátil entre sí. Es decir que se pueda comunicar una PDA con el Laptop y el celular para difundir la

información de los contactos personales entre sí, imprimir un e-mail desde un portátil, una PDA o un teléfono móvil entre otro.

Esta tecnología va encaminada a permitir el máximo uso de dispositivos posibles en el cuerpo de una persona.

Por esto y por muchas razones más se hace necesario que se profundice en el tratamiento de este tema de interés general.

1. RED DE ÁREA PERSONAL (PAN)

1.1 CONCEPTO

Una red de área personal, es la interconexión de dispositivos de información dentro de un rango de acción de una persona, que típicamente es de 10 metros. Por ejemplo una persona que posea una laptop, un asistente digital personal (PDA) y una impresora portátil, puede interconectarlos entre si sin necesidad de cables usando alguna clase de tecnología inalámbrica. Por lo general, esa clase de red de área personal podría ser interconectada sin cables a la Internet o a otras redes.

Este tipo de red es a la que llamamos WPAN. Estos conceptos son sinónimos debido a que la gran mayoría de las PAN son inalámbricas. Conceptualmente, la diferencia entre una PAN y una WLAN es que la primera tiende a ser centralizada alrededor de una persona mientras que la segunda es una red de área local que esta conectada sin hilos o cables y es utilizada por múltiples usuarios.

Una PAN es una tecnología que puede permitir la comunicación entre dispositivos de cómputo cargables (llevados en el cuerpo) y permitir el intercambio de información usando la conductividad eléctrica del cuerpo humano como una red de

datos. Por ejemplo dos personas que porten una tarjeta transmisora y receptora podrían intercambiar datos como el email, teléfono y dirección con una simple estrechada de manos, lo que se conoce como un linkup. Esto sería gracias a la salinidad natural del cuerpo humano la cual hace que sea un buen conductor de electricidad.

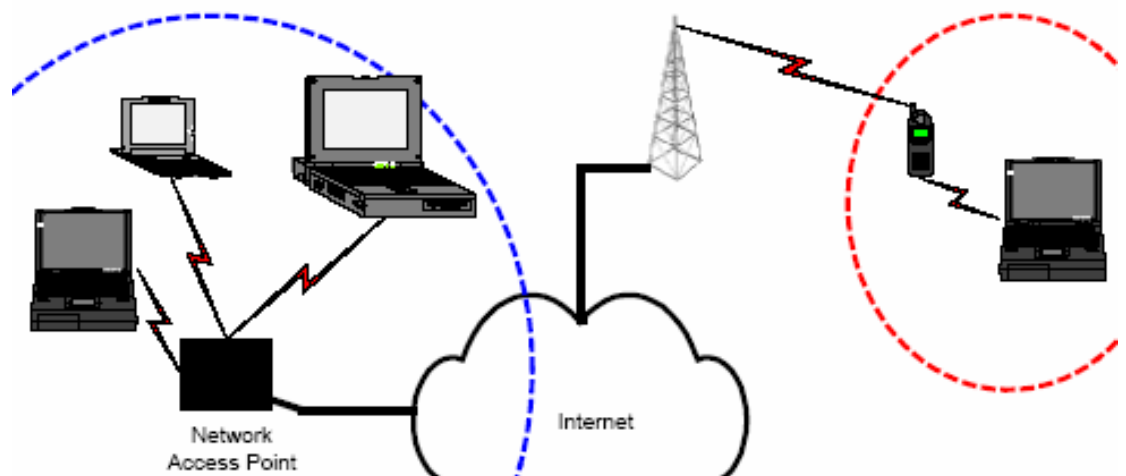
La primera persona en trabajar el concepto de una PAN fue Thomas Zimmerman y otros investigadores en el M.I.T's Media Lab y más adelante apoyado por el laboratorio de investigaciones de IBM. En su papel de investigador, Zimmerman explicó por qué el concepto podía ser útil: *“Cuando los dispositivos electrónicos se vuelven más pequeños, menor será el requerimiento de energía, lo cual los haría menos costosos. Tales dispositivos incluyen a los celulares, las PDA's, los video juegos de bolsillo entre otros. No hay actualmente un método para compartir datos entre esos dispositivos. Establecer una red con estos dispositivos puede reducir funciones de E/S redundantes y permitir nuevos servicios y convenios”*.

Gracias a los avances en tecnologías inalámbricas de corto alcance, así como la versatilidad de dispositivos personales, cada vez más personales e interoperables han hecho que esta reciente categoría de redes conocida como PAN, tenga gran aceptación en el mercado.

1.2 ESQUEMA DE CONECTIVIDAD DE DISPOSITIVOS

Precisamente, la tecnología inalámbrica Bluetooth, en la cual se basa esta monografía, se ha venido posicionando como un estándar global abierto para enlaces a través de ondas de radio, que ofrece conexiones inalámbricas entre computadoras portátiles, dispositivos de mano, teléfonos celulares y otros equipos móviles, y permite la transferencia remota de voz y datos. Estos avances han hecho posible el arranque de las redes personales inalámbricas, cuyo uso no estará limitado al hogar u oficina, sino a espacios públicos como aeropuertos, hoteles, etcétera, donde en un futuro cercano será posible desde un PDA o un celular contactar el servicio de abordaje de una aerolínea, confirmar el asiento y obtener pases de abordaje digitales, a través de un punto de acceso Bluetooth cercano (Figura 1).

Figura 1. Entorno Bluetooth



2. TECNOLOGÍA BLUETOOTH

2.1 NACIMIENTO

Bluetooth es un estándar para comunicaciones inalámbricas, la cual tiene como finalidad proporcionar conexiones instantáneas (ad hoc) para ambientes de comunicaciones tanto estáticos como móviles. Esta tecnología es de especificación abierta y su nombre proviene de un rey Vikingo de origen Danés llamado Harold Bluetooth.

Los inicios de Bluetooth se remontan al año de 1994, cuando la compañía Ericsson inició un estudio para investigar la viabilidad de una interfase vía radio, que fuese de bajo costo y consumo para la interconexión entre teléfonos móviles y otros accesorios con la intención de eliminar cables entre aparatos. El estudio partía de un largo proyecto que investigaba sobre unos multicomunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance, llamado *MC link*. Conforme este proyecto avanzaba se fue viendo claro que este tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenía como principal virtud el que se basaba en un chip de radio relativamente económico.

A comienzos de 1997, el interés de otros fabricantes de equipos portátiles fue aumentando, por lo que Ericsson vio que para que este sistema tuviera éxito, un gran número de equipos deberían estar equipados con ésta tecnología, por lo que a inicios de 1998 nace el Grupo de Interés Especial (**SIG**), formado por Ericsson, Nokia, IBM, Toshiba Corporation e Intel Corporation, a las que con posterioridad se les unieron 3Com Corporation, Lucent Technologies, Microsoft Corporation, Motorola Inc y otros cientos de compañías relacionadas con los sectores de la fabricación de componentes y las tecnologías de la información, la cuales son aproximadamente 1200 compañías.

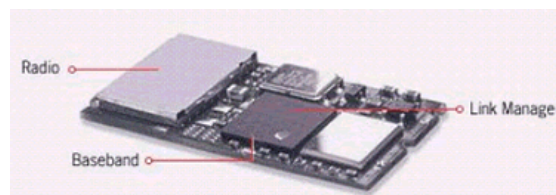
La meta primordial para los productos Bluetooth de primera generación fueron los entornos de la gente de negocios que viaja constantemente, por lo que se debía pensar en integrar el chip de radio Bluetooth en equipos como son los teléfonos móviles, auriculares, PDA'S y los PC'S portátiles, para así poder ser usados a nivel mundial

Para lograr tal objetivo, este protocolo se basa en enlaces radio de corto alcance, que posibilitan la creación de conexiones ad hoc entre dispositivos tanto móviles como fijos. Emplea la banda 2.4 GHz (ISM - Industrial, Científica y Médica), ya que no se necesita licencia para operar en ella porque es abierta. Solo en algunos países como Francia, España y Japón se presentan restricciones.

Bluetooth utiliza un sistema de transmisión FH/TDD (salto de frecuencia/división de tiempo duplex). La tasa binaria es de hasta 1 Mbps para los dispositivos de primera generación y de hasta 2 Mbps para los de segunda generación, utilizándose para enviar paquetes de pequeña longitud y un salto en frecuencia muy rápido (es decir utiliza la banda de frecuencia para ir transmitiendo paquetes de información lo que hace al sistema menos vulnerable a las interferencias, ofreciendo más seguridad y fiabilidad). La potencia de transmisión es de hasta 100 mW. La distancia nominal de enlace va desde los 10 cm a los 10 m, pudiéndose alcanzar los 100 sólo con adecuados amplificadores y antenas.

Un pequeño microchip Bluetooth (figura 2), que incorpora un radio transmisor, es introducido en los dispositivos digitales, por lo cual esta tecnología se encarga de realizar todas las conexiones de forma inmediata, sin utilizar ni un sólo centímetro de cable. Es decir, describe cómo pueden interconectarse todo tipo de dispositivos inalámbricos, ya sea en el hogar o en la oficina, utilizando una conexión de corto alcance.

Figura 2. Microchip Bluetooth



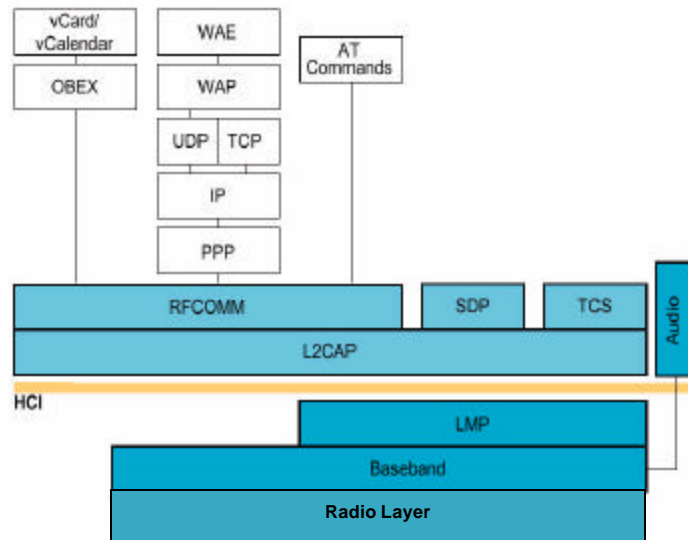
2.2 ESPECIFICACIONES DE LA TECNOLOGÍA

El objetivo final de la especificación es permitir que las aplicaciones funcionen unas con otras. Para conseguir este funcionamiento interactivo, las aplicaciones parejas (es decir, el correspondiente cliente y servidor de la aplicación) en dispositivos remotos deben funcionar sobre pilas idénticas de protocolos. La siguiente lista de protocolos es un ejemplo de una pila de protocolos (de arriba a abajo) que soporta la aplicación de intercambio de tarjetas de negocios:

vCard ? OBEX ? RFCOMM ? L2CAP ? Banda Base

Esta pila de protocolos contiene tanto un convenio para la representación de objetos internos, vCard, como protocolos de transporte 'sobre el aire', que serían el resto de la pila. Diferentes aplicaciones pueden funcionar sobre diferentes pilas de protocolos. Sin embargo, cada una de estas pilas de protocolos usa un enlace de datos y una capa física común. La Figura 3 muestra la pila completa de protocolos de Bluetooth tal como se define en la especificación. En la parte superior de la pila están las aplicaciones que soportan los modelos de uso de Bluetooth. No todas las aplicaciones hacen uso de todos los protocolos, sino que funcionan sobre uno o más cortes verticales de esta pila de protocolos. La Figura 3 muestra la relación en la cual cada protocolo utiliza los servicios de los demás protocolos cuando hay que transferir los datos, y también las relaciones con el resto de protocolos.

Figura 3. Niveles Bluetooth



2.2.1 Enlace de Radio

Bluetooth ha sido diseñado para operar en un ambiente de radio frecuencia ruidoso, utiliza un esquema de reconocimiento rápido y saltos de frecuencia para garantizar la robustez del enlace. Como ya se ha mencionado, Bluetooth opera en la banda de frecuencia de 2.4 GHz, libre para ISM (Industrial, Científica, Medica). Los módulos de radio Bluetooth eliminan la interferencia con otras señales saltando a una nueva frecuencia inmediatamente después de transmitir o recibir un paquete. Comparado con otros sistemas que operan en la misma frecuencia, Bluetooth salta más rápido y usa paquetes más pequeños. Esto hace que sea más robusto que otros sistemas. Además, de esta forma también se limita el impacto de los hornos de microondas, tanto domésticos como profesionales. El empleo de

una corrección de error hacia delante (FEC, *Forward Correction Error*) reduce el efecto del ruido aleatorio en enlaces de larga distancia.

2.2.2 Banda Base

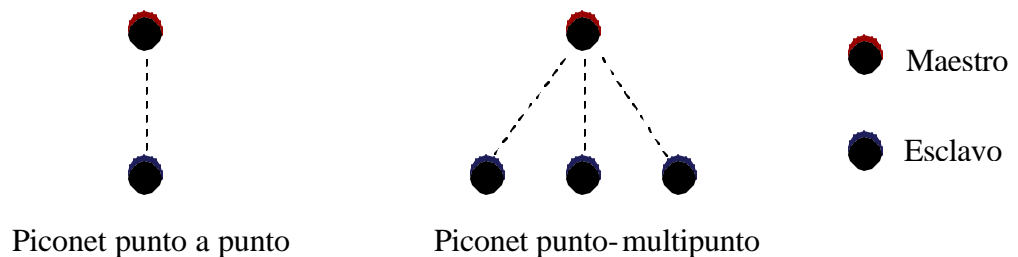
La banda base es la capa física de Bluetooth. Se encarga del manejo de los canales físicos y los enlaces así como otros servicios como corrección de errores, selección de saltos, formateo de datos y seguridad.

El protocolo Bluetooth utiliza una combinación de conmutación de circuitos y paquetes. Los slots pueden ser reservados para paquetes síncronos. Bluetooth puede soportar un canal de datos asíncronos la vez que 3 canales de voz síncronos o un canal que soporte simultáneamente un canal síncrono y asíncrono. Cada canal de voz permite un canal síncrono de 64 Kbps en cada dirección. El canal asíncrono permite un enlace asimétrico de 723.2 Kbps y 57.6 Kbps en la respuesta, o un enlace simétrico de 433.9 Kbps. Los paquetes de voz no se retransmiten, ya que el método de codificación (CVSD) permite que la voz sea audible incluso con altos niveles de ruido.

El sistema Bluetooth proporciona conexiones punto a punto (solamente entre dos unidades Bluetooth) o conexiones multipunto. En esta última conexión el canal es compartido entre diversas unidades. Dos o más unidades compartiendo un mismo canal forman una **piconet (figura 4)**. Una unidad Bluetooth actúa como maestro

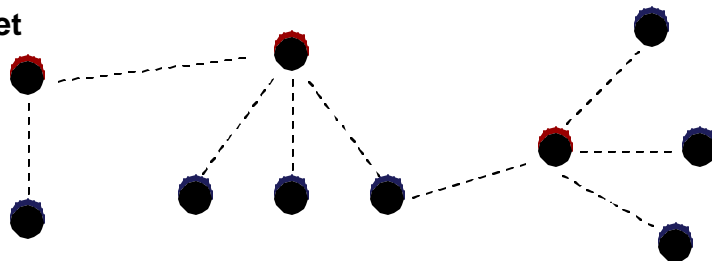
en la *piconet*, mientras que las otras como esclavos. Solo pueden hacer parte de esta 7 esclavos. Muchos más esclavos pueden permanecer en estado estacionario (*parked*) mientras entablan comunicación con el maestro. Estas unidades no pueden estar activas en el canal pero se mantienen sincronizadas con el maestro. Para ambos casos, activo y en modo estacionario, el canal permanece controlado por la unidad maestra.

Figura 4



Múltiples *piconets* conforman lo que se conoce como una **scatternet** (figura 5). Cada piconet solo puede tener un maestro. Cada esclavo puede participar en diferentes *piconets* basado en el esquema de la división de tiempo full duplex. Además de que un maestro en una piconet puede ser esclavo en otra distinta. Las *piconets* no estarán sincronizadas en frecuencia. Cada una de ellas maneja su propio canal de saltos.

Figura 5. Scatternet



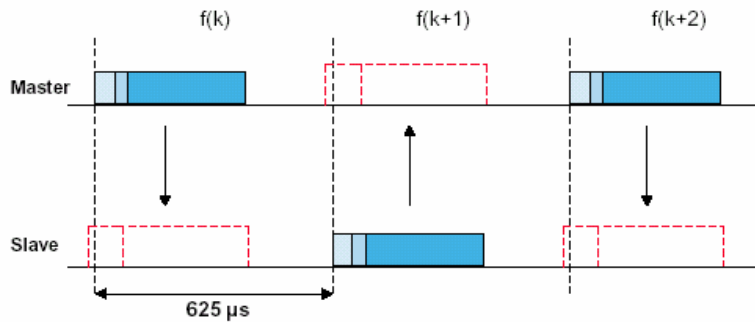
2.2.2.1 Canal físico

A la señal de radio se le ha añadido una expansión del espectro para facilitar la operación a niveles de potencia de más de 100mW. Se producen además 79 saltos en frecuencia desplazados 1MHz, de 2.402 GHz a 2.480 GHz. Debido a regulaciones locales, el ancho de banda se ve reducido en Francia, España y Japón. Esto es gestionado por el software interno. La frecuencia máxima de saltos es de 1600 por segundo. La distancia nominal del enlace está comprendida entre 10 cm y 10 m, pero se puede aumentar a más de 100 m elevando la potencia de transmisión.

El canal está dividido en *slots* de tiempo, en donde cada *slot* tiene un tamaño de 625 μ s. Lo cual corresponde a un salto de radio frecuencia (RF). Saltos consecutivos corresponden a diferentes saltos de radio frecuencia. Los *slots* de tiempo son numerados de acuerdo al reloj del dispositivo maestro de la *piconet*. En estos *slots* de tiempo el maestro y esclavo pueden transmitir paquetes.

El esquema de división de tiempo es usado cuando tanto esclavo como maestro transmiten de manera alternativa. El maestro inicia la comunicación únicamente en los slots de tiempo par, mientras que el esclavo lo hace en los impares (figura 6). El inicio del paquete estará alineado con el inicio del *slot*.

Figura 6



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, ésta primera debe añadir un ajuste a su propio reloj nativo y así poder compartir la misma portadora de salto.

2.2.2.2 Enlace Físico

Entre maestro y esclavo(s) se pueden establecer diferentes tipos de enlace. Para mayor precisión hay dos definidos:

- Orientados a conexión (síncronos) o SCO: Este es un enlace punto a punto entre una maestro y un esclavo de la piconet. El maestro mantiene el enlace SCO utilizando *slots* reservados en intervalos regulares

(conmutación de circuitos). Un enlace SCO porta principalmente información de voz. El maestro puede soportar 3 enlaces SCO simultáneos al mismo o a diferentes esclavos. El esclavo solo puede soportar 3 enlaces desde un mismo maestro o dos enlaces SCO si éstos se originan de diferentes maestros. Si el esclavo falla al decodificar la dirección del encabezado del paquete, puede devolver un paquete SCO en el *slot* SCO reservado. Los paquetes SCO son utilizados para transmisiones de voz a 64 Kbps.

- No orientados a conexión (asíncronos) o ACL: Este es un enlace punto-multipunto entre el maestro y todos los esclavos que participan en la piconet. En los *slots* no reservados por los enlaces SCO, el maestro puede establecer un enlace ACL por esclavo, incluyendo al que ya tiene un enlace SCO (conmutación de paquetes). Solo puede existir un enlace ACL entre esclavo y maestro. Para más paquetes ACL se aplica la retransmisión de paquetes. Los paquetes no direccionados a ningún esclavo son considerados como paquetes broadcast y son leídos por todos los esclavos.

2.2.2.3 Paquetes

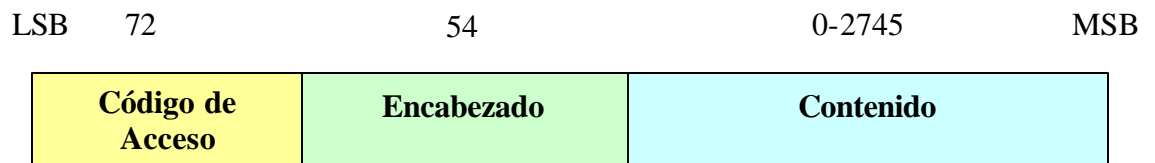
El ordenamiento de los bits cuando se definen los paquetes a ser transmitidos, cuenta con las siguientes reglas:

- El bit menos significativo (LSB) corresponde al bit b_0 .
- El LSB es el primer bit a ser transmitido por el aire.
- En las ilustraciones que utiliza la tecnología Bluetooth, el LSB siempre se mostrará del lado izquierdo.

Cualquier dato a transmitir por un canal en una piconet o una scatternet es convertido en paquetes. La capa banda Base cuenta con 16 tipos de paquetes. Todos los niveles superiores utilizan estos paquetes para componer mensajes de alto nivel o PDU (protocol data unit).

El formato general de un paquete de datos en Bluetooth es el siguiente (figura 7)

Figura 7

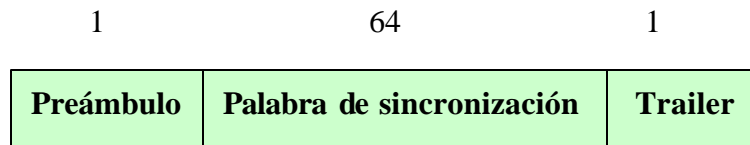


2.2.2.3.1 Código de Acceso

Todo paquete comienza con un código de acceso. El código de acceso es utilizado para sincronización, compensación e identificación de los dispositivos o

unidades Bluetooth. Consta de un campo de preámbulo utilizado para la compensación, una palabra de sincronización y un campo *trailer* que se añade si le sigue la parte de encabezado (figura 8).

Figura 8



El código de acceso tiene 72 bits si va precedido del encabezado, sino es de 68 bits. Hay tres clases de códigos de acceso (Tabla 1):

CLASE	DESCRIPCION
Código de acceso de canal (CAC)	Este código identifica una <i>piconet</i> . El código está incluido en todos los paquetes intercambiados en el canal de la <i>piconet</i> .
Código de acceso de dispositivo (DAC)	Es utilizado para paginación.
Código de acceso de búsqueda (IAC)	Es utilizado con el propósito de realizar preguntas de control. Hay dos variaciones de este tipo de acceso: El general (GIAC) para descubrir que otros dispositivos se encuentran en un rango y el dedicado (DIAC) que es común para grupos de unidades Bluetooth que comparten características similares.

Tabla 1. Clases de códigos de acceso

2.2.2.3.2 Encabezado

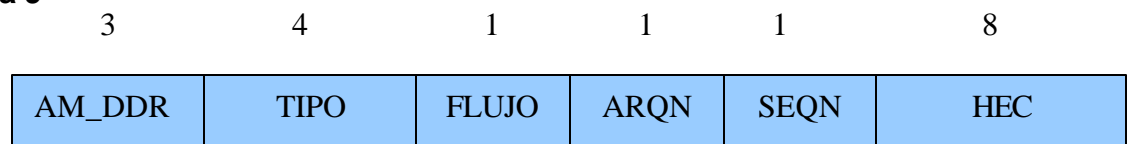
El encabezado ejerce funciones de control de enlace (LC) y consiste de 6 campos (figura 9):

- **AM_DDR:** Representa la dirección de un dispositivo activo en la *piconet* y es utilizado para distinguirlo de los demás miembros dentro de esta. Para identificar cada esclavo separadamente dentro de la *piconet*, cada uno de estos tiene asignada temporalmente una dirección de 3 bits.
- **Tipo:** Existen 16 diferentes tipos de paquetes. Este campo consta de 4 bits que distinguen el tipo de paquete a utilizarse. El tipo de paquete depende de la clase conexión que se establezca entre maestro y esclavo (ACL, SCO). El campo Tipo revela cuántos slots ocupará el paquete.
- **Flujo:** Este campo es utilizado para el control de flujo de los paquetes en enlaces ACL. Consta de un bit. Cuando el buffer en el receptor de un enlace ACL se encuentra lleno y no ha sido desocupado, una señal de *stop* (Flujo=0) es regresada para indicar que se detenga la transmisión temporalmente. Cuando el buffer está desocupado se envía una señal de reinicio o *go* (Flujo=1). Cuando no se recibe ningún paquete o el encabezado recibido contiene un error la señal *go* es asumida implícitamente. En este caso el

esclavo podrá recibir un nuevo paquete corregido a pesar de que el buffer no está vacío.

- **ARQN:** Campo que consta de un bit para informar si la carga o contenido transmitido con CRC es recibido o no correctamente. Si su valor es uno, indica que se recibió sin problemas y se conoce como ACK. Si el valor es cero es lo contrario y se conoce como NAK.
- **SEQN:** El bit de este campo proporciona un esquema de secuenciamiento para el orden en el envío de los datos. Para cada nuevo paquete transmitido que contenga datos con CRC, el bit SEQN es invertido. Esto sirve para filtrar las retransmisiones en el destino; si una retransmisión ocurre debido a un ACK fallido, el destino recibe el mismo paquete dos veces. Entonces al comparar el SEQN de paquetes consecutivos, las retransmisiones correctamente recibidas pueden ser desechadas.
- **HEC:** Cada encabezado cuenta con un código de comprobación de error (HEC) de 8 bits. Este es un código redundante cíclico (CRC) que detecta errores en el encabezado.

Figura 9



2.2.2.3.3 Tipos de paquetes

Como ya se había mencionado los tipos de paquetes de una *piconet* están relacionados con el tipo de enlace físico que se esté utilizando, ya sea ACL o SCO. Para cada uno de estos enlaces pueden ser definidos 12 tipos de paquetes. Cuatro paquetes de control son comunes para ambos tipos de enlace, por lo cual es el tipo de código es único indistintamente de que el enlace sea ACL o SCO.

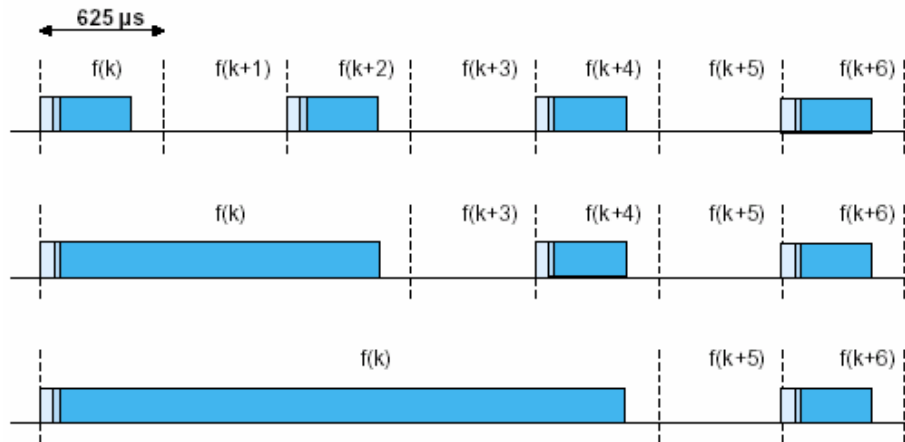
Hay cuatro tipos de paquetes de control comunes a saber (Tabla 2):

TIPO	DESCRIPCION
Paquete ID	Consiste en el DAC (código de acceso de dispositivo) o en el IAC (código de acceso de búsqueda). Este paquete es utilizado en la paginación, búsqueda y rutinas de respuesta.
Paquete NULL	Este paquete contiene el código de acceso y un encabezado de paquete. Se utiliza cuando se tiene que transmitir información de control de enlace a la fuente con respecto al resultado de una transmisión exitosa (ARQN) o el estado el buffer en un enlace ACL.
Paquete POLL	Es similar al <i>Null</i> , excepto que necesita de una confirmación por parte del receptor. Los dispositivos maestros utilizan el paquete <i>poll</i> para forzar a los esclavos a responder.
Paquete FHS	Se utiliza para intercambiar información del reloj y de identificación entre unidades. Contiene toda la información necesaria para mantener a dos unidades sincronizadas en el salto de frecuencias.

Tabla 2. Tipos de paquetes

Los 12 tipos de paquetes restantes son utilizados para definir paquetes para servicios síncronos y asíncronos. Estos paquetes se pueden definir dentro de tres clases: paquetes que caben en 1 *slot*, paquetes de 3 *slots* y paquetes de 5 *slots*. Los paquetes multislot se envían por un sólo canal, es decir, utilizan la misma banda de frecuencias para transmitir y no realizan salto en frecuencias. La frecuencia utilizada en el primer *slot* es la que se utiliza para retransmitir en los otros *slots*. Una vez que se termina de transmitir todo el paquete, se cambia de frecuencia respecto a la información actual del reloj (figura 10).

Figura 10



2.2.2.3.4 Campo Contenido

Se distinguen dos campos en el campo contenido: el campo de voz (síncrono) y el campo de datos (asíncrono). Los paquetes ACL sólo tienen campos asíncronos y

los paquetes SCO solo los síncronos. La excepción se presenta en los paquetes DV (voz y datos) que poseen los dos campos. El campo de datos consta de 3 partes: un encabezado que especifica cual es el canal lógico, el control de flujo en los canales lógicos y un indicador de tamaño de contenido; un cuerpo de contenido que incluye información del host del usuario y determina la efectividad del procesamiento del usuario; por último un campo CRC para las retransmisiones de paquetes.

2.2.2.4 Corrección de errores

Bluetooth define dos tipos de corrección de errores: FEC y retransmisión de paquetes. Para FEC se soportan tasas de 1/3 y de 2/3. El propósito de la utilización de estos esquemas es la reducción de las retransmisiones producidas por errores. El encabezado de un paquete siempre está protegido por FEC de 1/3.

- **FEC con tasa de 1/3:** Se implementa repitiendo el bit 3 veces. Por ejemplo b_0 b_0 b_1 b_1 b_1 . Se utiliza como se había dicho en los encabezados y además puede ser usado en el campo de datos de usuario de paquetes en enlaces SCO.

- **FEC con tasa de 2/3:** Es un esquema abreviado del código de Hamming. Este código puede aplicarse tanto al campo de datos de usuario de paquetes síncronos (en enlaces SCO) como al campo de datos de usuario de paquetes asíncronos (en enlaces ACL). Codifica con códigos de 10 y 15 bits.
- **ARQ:** Su uso es para los enlaces ACL. Los paquetes se transmiten y retransmiten hasta que se tenga reconocimiento de una transmisión correcta por parte del receptor o una ocurrencia de tiempo de espera agotado. Esta información está incluida en el encabezado del paquete devuelto y se añade un código CRC al paquete para comprobar errores.

2.2.2.5 Canales Lógicos

Bluetooth tiene cinco canales lógicos que pueden ser utilizados para transmitir diferente tipo de información y comunican la banda base con las capas superiores, estos son:

- **LC (Link Control):** Este canal lleva información a nivel de enlace como ARQ, control de flujo. Cada paquete lleva un canal LC en su encabezado, a excepción del paquete ID que no posee encabezado.

- LM (Link Manager): Lleva información de control que intercambian los gestores de enlace del maestro y del esclavo. Se utiliza en enlaces ACL y SCO.
- UA (User Asynchronous Data): Transporta datos de usuario asíncrono correspondientes al protocolo L2CAP.
- UI (User Isochronous Data): Transporta datos de usuario isócronos y es soportado por los paquetes de comienzo de temporización en los niveles más altos.
- US (User Synchronous Data): Es utilizado en los enlaces SCO.

2.2.2.6 Rutinas de transmisión y recepción

La rutina de transmisión se realiza de manera separada para el enlace ACL (el maestro tiene un buffer para cada esclavo) y para el enlace SCO (varios buffers por cada esclavo). Tanto el buffer ACL como el SCO consta de dos registros FIFO. Uno puede ser accedido y leído por el controlador de Bluetooth para componer los diferentes paquetes mientras que el otro registro tan sólo puede ser accedido por LMP para cargar nueva información.

La rutina de recepción también se realiza de manera separada para los enlaces ACL y SCO. Para el ACL solamente existe un buffer de recepción que es compartido por todos los esclavos, mientras que para el SCO se utilizan uno o más buffers. El buffer ACL consiste en dos registros FIFO, uno al que puede acceder y cargar la información del controlador de Bluetooth para acceder al contenido, y otro registro, únicamente accesible por LMP para leer la información previa al contenido. Por su parte, el buffer SCO consta de dos registros FIFO, uno de los cuales se llena de información de voz, mientras que el otro registro sólo puede acceder a la unidad de procesado de voz.

2.2.2.7 Canal de Control

A continuación se describe cómo se establece el canal de una *piconet* y cómo las unidades Bluetooth pueden ser adicionadas o retiradas de ésta. Varios estados de las unidades Bluetooth de la piconet se definen para apoyar estas funciones. Además la operación de varias *piconets* compartiendo la misma área, lo cual conocemos como scatternet será tratada.

2.2.2.7.1 Definición maestro-esclavo

El canal de una *piconet* es manejado completamente por el maestro. La dirección del dispositivo Bluetooth (BD_ADDR) del maestro determina la frecuencia de salto y el código de acceso al canal; el reloj del sistema del maestro determina la fase

en los saltos de frecuencia y establece la sincronización. Además de esto controla el tráfico en el canal bajo un esquema de interrogación.

Por definición el maestro Bluetooth está representado por aquel dispositivo que inicia la conexión con una o más unidades.

2.2.2.7.2 Estados del controlador de enlace

El controlador de enlace de Bluetooth opera en dos estados principalmente:

- **Standby:** Es el estado por defecto con menor gasto de energía en la unidad Bluetooth. Sólo funciona el reloj interno y no hay interacciones con ningún otro dispositivo.
- **Conexión (Connection):** El maestro y el esclavo pueden intercambiar paquetes, usando el código de acceso al canal y el reloj del maestro Bluetooth.

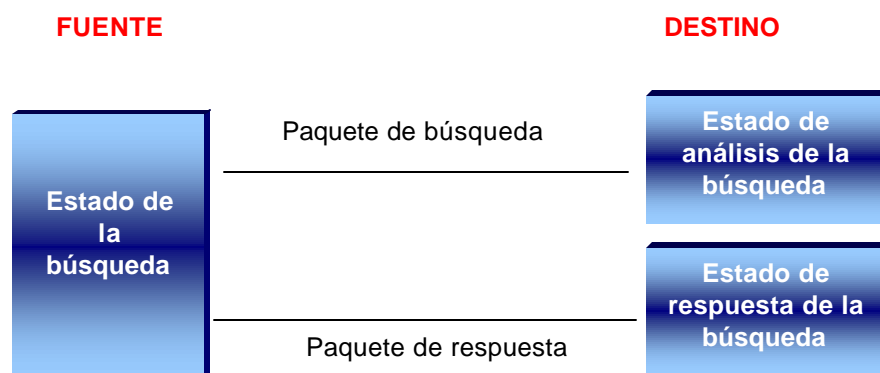
Existen 7 subestados que se utilizan para adicionar esclavos o hacer conexiones en la *piconet*. Page (paginación), Page Scan (análisis de la paginación), Inquiry (búsqueda), Inquiry Scan (estado de la búsqueda), Master Reponse (respuesta del maestro), Slave Reponse (respuesta del esclavo) e Inquiry Response (respuesta de la búsqueda)

2.2.2.7.3 Establecimiento de la conexión

Por lo general, el establecimiento de la conexión entre dos dispositivos ocurre de la siguiente manera: Si no se conoce nada sobre el dispositivo remoto se realiza el proceso de búsqueda (inquiry) y luego el de paginación (page). Si se conoce la existencia de un dispositivo solo se realiza el proceso de paginación.

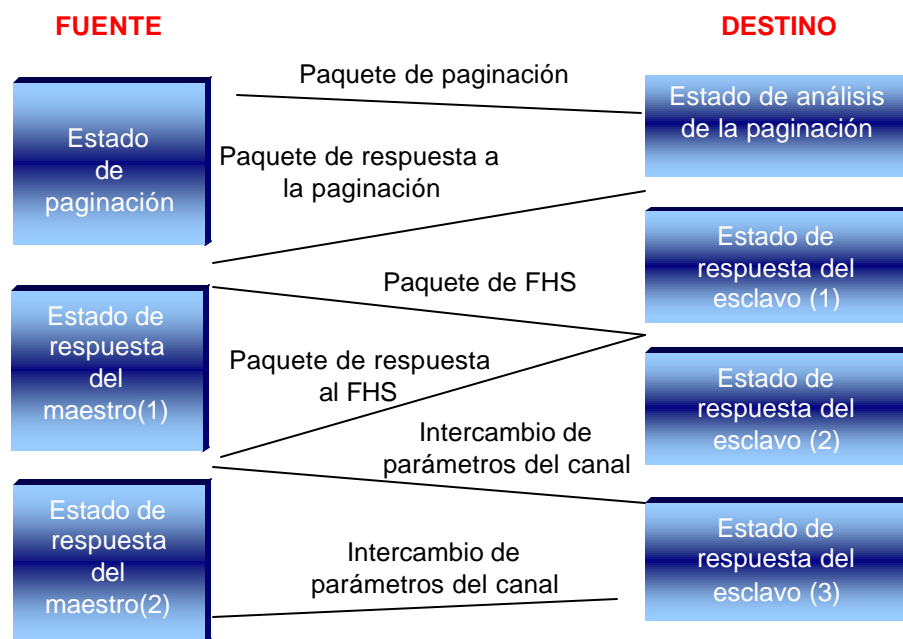
- **Proceso de búsqueda (figura 11):** Este proceso permite descubrir un dispositivo o dispositivos que se encuentren dentro de su rango de cobertura, determina las direcciones y los relojes de los mismos. El proceso de búsqueda implica a un dispositivo fuente que envía los paquetes de búsqueda (estado de búsqueda) y recibe la respuesta a su búsqueda. El dispositivo destino, que recibe los paquetes de búsqueda, estará en el estado de análisis de la búsqueda en el cual está atento a recibir dichos paquetes. Luego esta unidad entra en el estado de respuesta de la búsqueda y envía una contestación a la fuente. Ya finalizado este proceso se puede establecer una conexión utilizando el procedimiento de paginación.

Figura 11. Proceso de búsqueda



- Proceso de paginación:** A través de este se puede establecer la conexión verdadera. Este proceso funciona de manera similar al proceso de búsqueda. Sólo necesita la dirección del dispositivo Bluetooth para establecer la conexión. El conocimiento del reloj acelera el proceso de establecimiento de conexión. El dispositivo que establece la conexión lleva a cabo el procedimiento de paginación y será el maestro de la *piconet*. En la figura 12 se ilustra como es este proceso.

Figura 12. Proceso de paginación



- Un dispositivo (la fuente) pagina otro dispositivo (el destino). Estado Page
- El destino recibe la página. Estado Page Scan

- El destino envía una respuesta a la fuente. Estado Slave Response

- La fuente envía un paquete FHS al destino. Estado Master Response

- El destino envía su segunda respuesta a la fuente. Estado Slave Response

- El destino y la fuente intercambian entonces los parámetros del canal fuente. Estado Master Response Response & Slave Resp.

- El estado Connection comienza con un paquete POLL enviado por el maestro para verificar que el esclavo ha cambiado al salto de frecuencia de canal y temporización del maestro. El esclavo puede responder con cualquier tipo de paquete

2.2.2.7.4 Modos de conexión

Un dispositivo Bluetooth en estado de conexión puede estar en cualquiera de los modos explicados en la tabla 3.

MODOS DE CONEXION	DESCRIPCION
Active	El dispositivo o unidad participa activamente del canal. El maestro planifica la transmisión con base a las peticiones de tráfico hacia y desde los diferentes esclavos. Además, mantiene a los esclavos sincronizados al canal. Los esclavos activos escuchan los <i>slots</i> maestro-a-esclavo esperando paquetes.
Hold	El maestro tiene la capacidad de colocar un esclavo en modo <i>hold</i> , donde sólo un reloj interno avanza. Los esclavos también pueden enviar una petición de colocación en este modo. La transferencia de datos se reinicia automáticamente apenas salen de este estado. Tiene un ciclo de trabajo intermedio entre los tres modos de energía (<i>hold</i> , <i>park</i> , <i>sniff</i>).
Park	Un dispositivo bluetooth se sincroniza con la <i>piconet</i> pero no participa del tráfico. En este modo los dispositivos dejan su MAC (AM_ADDR) y esporádicamente escuchan el tráfico del maestro para volverse a sincronizar y recibir mensajes de broadcast.
Sniff	Un esclavo escucha de la <i>piconet</i> con una tasa reducida, reduciendo así su ciclo de trabajo. El intervalo de <i>Sniff</i> es programable y depende de la aplicación.

Tabla 3. Modos de conexión Bluetooth

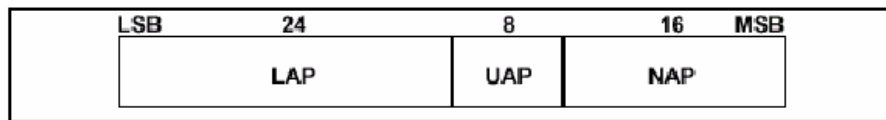
2.2.2.8 Direccionamiento de los dispositivos

Hay cuatro formas de direccionamiento posible para los dispositivos Bluetooth:

- **BD_ADDR (Bluetooth device address o dirección de dispositivo Bluetooth):** cada transmisor Bluetooth posee una única dirección de 48 bits

(figura 13). Está dividida en un campo de 24 bits LAP (Lower Acces Part), un campo de 8 bits UAP (Upper Access Part) y un campo de 16 bits NAP (Non-significant Access Part). Se pueden utilizar 2^{32} direcciones (24 bits LAP + 8 bits UAP).

Figura 13. Dirección básica de un dispositivo Bluetooth



Además de esta dirección se pueden asignar otras tres clases de direcciones:

- **AM_ADDR (dirección de miembro activo):** Es un número de 3 bits. Es solamente válida tan pronto como el dispositivo esclavo está activo en el canal. Algunas veces es llamado la dirección MAC de una unidad Bluetooth.
- **PM_ADDR (dirección de un miembro aparcado (park)):** Se asigna solo si el esclavo está en modo *park*.
- **AR_ADDR (petición de dirección de acceso):** Esta dirección es usada por los esclavos en modo de parqueo para determinar que la mitad del *slot*

de la ventana de acceso esclavo-maestro es válida para enviar mensajes de petición de acceso.

2.2.2.9 Seguridad

Los datos transmitidos por los dispositivos Bluetooth son, en general, objetivos claros para posibles espías. Esto se debe a que muchos de estos dispositivos tienen la característica de ser del tipo agendas personales, en los que se almacenan informaciones del tipo citas, contraseñas, teléfonos, direcciones, etc., en poca palabras cosas que son susceptibles de ser espiadas.

Además se debe adicionar el hecho de que utiliza radiofrecuencia, con lo que no podemos limitar el alcance de la señal y puede haber un posible atacante escuchando las señales emitidas por estos dispositivos.

El Perfil de Acceso Genérico de Bluetooth, que es el marco en el cual se centran los demás perfiles, define tres modos de seguridad relacionados en la siguiente tabla (4):

MODO DE SEGURIDAD	DESCRIPCION
1	Es un modo no seguro. No se realiza ninguna tarea de seguridad.
2	Conocido como Seguridad Impuesta Nivel de Servicio, es el modo en el cual el dispositivo empieza a utilizar las características de seguridad en las capas de nivel superior. Son las aplicaciones las que deciden si quieren utilizar las características de seguridad que ofrece el protocolo.
3	Se conoce como el modo de Seguridad Impuesto a Nivel de Enlace, en el cual el dispositivo inicia el procedimiento de seguridad antes de que el canal haya sido establecido (capas de nivel inferior).

Tabla 4. Modos de seguridad

Además existen dos posibilidades en el acceso de los dispositivos a diferentes servicios: *Dispositivos de confianza* los cuales tienen acceso sin restricción alguna a todos los servicios y los de *no confianza* que tienen acceso limitado.

Los servicios también pueden ser definidos en tres niveles de seguridad:

- **Servicios abiertos:** Cualquier dispositivo puede acceder a ellos.
- **Servicios que requieren solo autenticación:** Cualquier dispositivo que haya sido autenticado puede acceder a ellos, ya que ha demostrado que comparte una clave de enlace con el proveedor del servicio.
- **Servicios que requieren autenticación y autorización:** Solo acceden a estos servicios los dispositivos de confianza, quedando grabados en la base de datos del servidor.

Para conseguir seguridad, tanto en el acceso a otros dispositivos Bluetooth como en la transmisión de la información entre ellos, es necesario un complejo entramado de seguridad que afiance estos dos aspectos. Para mantener la seguridad a nivel de enlace se utilizan cuatro parámetros:

- La dirección del dispositivo Bluetooth, BD_ADDR. Tiene una longitud de 48 bits.
- La clave de usuario privado de autenticación. Tiene una longitud fija de 128 bits
- La clave de usuario privado de cifrado. Esta se obtiene a partir de la autenticación., proceso durante el cual tiene una longitud variable de entre 8 y 128 bits.
- Un número aleatorio, RAND. Viene de un proceso aleatorio que tiene lugar en la unidad Bluetooth.

2.2.3 Protocolo de Administración de Enlace (Link Manager Protocol, LMP)

El Administrador de Enlace (LM) se encarga del establecimiento del enlace, la autenticación, la configuración del enlace, control de tamaño de paquetes, control de potencia y los ciclos de trabajo en la transmisión de radio, control de la calidad de servicio y la conmutación maestro-esclavo. El LM descubre otros

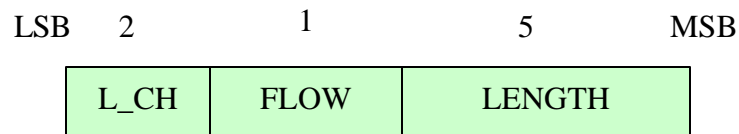
administradores de enlace remotos y logra la comunicación con ellos gracias al Protocolo de Administración de Enlace (LMP). El Administrador de Enlace utiliza los servicios de apoyo del Controlador de Enlace (LC) para poder proporcionar servicios.

Los mensajes del Administrador de Enlace tienen mayor prioridad que los datos de usuario. Esto significa que si LM necesita enviar un mensaje, no deberá retrasarse debido al tráfico L2CAP (datos), aunque podría darse el caso si se tienen numerosas retransmisiones de paquetes de la Banda Base. Según las especificaciones, LC nos debe proporcionar un enlace fiable.

2.2.3.1 Formato LMP

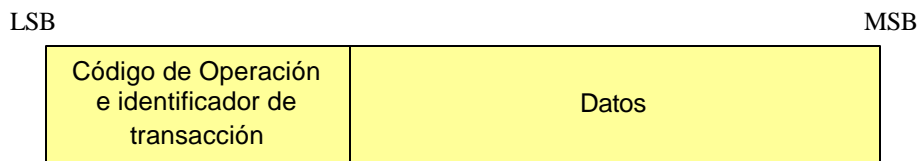
Las PDU's LM siempre se envían como paquetes de un único *slot*, y el encabezado de datos es de un byte (figura 14), siendo los dos bits menos significativos (campo L_CH) los que determinan el canal lógico.

Figura 14. Encabezado de un paquete de datos de un *slot* simple



El bit *Flow* siempre tiene valor de 1 y es ignorado en el lado receptor. Cada PDU tiene asignado un código de operación de 7 bits que identifica de forma única los diferentes tipos de PDUs (figura 15). Este código de operación y un bit de identificación de transacción van en el primer byte del cuerpo del contenido. El bit de identificación está en el LSB, y si su valor es 0 la PDU corresponde a una transacción iniciada por el maestro y si es 1 por el esclavo. Si la PDU contiene uno o más parámetros estos son colocados en el segundo byte al comienzo del campo contenido. El número de bytes utilizados depende de la longitud de los parámetros.

Figura 15. Cuerpo del contenido cuando se envía una PDU



No todas las PDUs son obligatorias, sino que existe un conjunto de éstas que son opcionales. En este caso, el Administrador del Enlace no tiene por qué ser capaz de transmitir una PDU opcional. Debe reconocer todas las PDUs opcionales que reciba, y si se requiere respuesta, enviar una válida de acuerdo a los procedimientos indicados en las especificaciones.

El destino y origen de una PDU se determinan gracias a la dirección *AM_ADDR*, que como ya se había explicado anteriormente, se trata de 3 bits que indican el número de esclavo activo dentro de la piconet.

2.2.3.2 Procedimientos LMP

LMP realiza una gran cantidad de procedimientos relacionados con la gestión de las *piconets* y la seguridad. En la Tabla 5 se relacionan algunos de estos.

NOMBRE	DESCRIPCIÓN
Respuesta general	Se usan como mensajes de respuesta a otras PDUs en diferentes procedimientos, conteniendo el código de operación del mensaje al que se responde.
Autenticación	El verificador envía al demandante un código que contiene un número al azar. El demandante calcula una respuesta, que es devuelta al verificador. Si es correcta dos aparatos compartirán la clave secreta.
Petición de ajuste del reloj	Cuándo un esclavo recibe el paquete FHS, calcula la diferencia entre su reloj y el del maestro que va incluido en el campo de contenido del paquete. La desviación del reloj se actualiza también cada vez que se recibe un paquete del maestro. El esclavo puede solicitar esta desviación de reloj en cualquier momento la conexión.
Calidad del servicio	Un intervalo de sondeo (poll), se usa para la asignación de ancho de banda y control de latencia. Además, se negocian el número de repeticiones para paquetes broadcast.
Supervisión del enlace	Cada enlace de Bluetooth tiene un reloj que se usa para la supervisión del enlace y para detectar la pérdida del enlace causada por dispositivos que salen de la cobertura, caída de potencia de un aparato, u otros casos semejantes de fallo.
Manejo de errores	Si el Administrador del Enlace recibe una PDU con código de operación no reconocido, o si recibe una PDU con parámetros inválidos responde con un comando de no aceptación especificando la razón. Si el tiempo máximo de la respuesta se excede o si se detecta pérdida del enlace, la parte que espera la respuesta concluirá que el procedimiento ha terminado fallidamente.

Tabla 5. Procedimientos LMP

2.2.4 Control Lógico de Enlace y Protocolo de Adaptación

El Control Lógico de Enlace y Protocolo de Adaptación (L2CAP) se encuentra por encima de la Banda Base y hace parte de la capa de enlace de datos. L2CAP proporciona servicios de datos orientados y no orientados a conexión a protocolos de capa superior con capacidad de multiplexación, segmentación y reensamble y administración de grupos. L2CAP permite a los protocolos de capa superior y a las aplicaciones transmitir y recibir paquetes de 64 Kb de longitud.

La especificación L2CAP se define solo para los enlaces ACL vistos en la Banda Base. Para los enlaces SCO no hay ninguna definición.

L2CAP tiene varios requerimientos funcionales entre los cuales encontramos la multiplexación de protocolo, segmentación y reensamble de paquetes, calidad de servicio, y el manejo de grupos.

2.2.4.1 Operaciones Generales

L2CAP se basa en el concepto de *canales*. Cada uno de los puntos finales de un canal L2CAP hace referencia al *identificador de Canal*.

- **Identificadores de Canal:** Los identificadores de canal (CIDs) son los nombres locales que representan un punto final lógico del canal en el

dispositivo. La tarea de CID es relativa a un dispositivo determinado y este puede asignar CIDs independientemente de otros dispositivos (con excepción de los CID reservados). Así, un dispositivo local puede tener el mismo valor de CID para distintos dispositivos remotos, pero el dispositivo local debe asociar únicamente cada CID remoto con un dispositivo diferente.

- **Operación entre dispositivos:** Los canales de datos orientados a conexión representan una conexión entre dos dispositivos, donde un CID identifica cada punto final del canal. Los canales sin conexión restringen el flujo de datos a una sola dirección.

Hay también varios CIDs reservados para propósitos especiales, como el canal de señalización, que se usa para crear y establecer los canales de datos orientados a conexión y para negociar los cambios en las características de estos canales. El soporte de un canal de señalización dentro de una entidad L2CAP es obligatorio. Otro CID se reserva para todo tráfico entrante de datos sin conexión.

- **Operaciones entre capas:** Las implementaciones L2CAP siguen la arquitectura general descrita de la siguiente forma: Deben transferir datos entre los protocolos de nivel superior y los de nivel inferior; cada

implementación debe soportar un conjunto de comandos de señalización para utilizar entre implementaciones L2CAP y por último estas implementaciones deben estar preparadas para aceptar ciertos tipos de eventos de capas inferiores y generar eventos hacia capas superiores.

- **Segmentación y reensamble:** Las operaciones de segmentación y reensamble son utilizadas para mejorar la eficiencia al soportar una unidad máxima de transmisión (MTU) de mayor tamaño que el paquete más grande de Banda Base. Todos los paquetes L2CAP podrían ser segmentados para transferirlos sobre paquetes de Banda Base. El protocolo no realiza ninguna operación de segmentación y reensamble pero el formato del paquete permite la adaptación a tamaños de trama física más pequeños.
- **Primitivas del servicio:** Varios servicios son ofrecidos por L2CAP en términos de primitivas y parámetros de servicio. El interfaz del servicio es requerido para la realización de pruebas. Dentro de estas primitivas encontramos:
 - Conexión: ajuste, configuración, desconexión.
 - Datos: lectura, escritura.

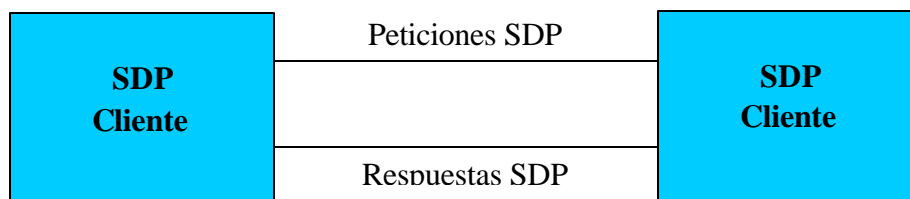
- Grupos: crear, cerrar, agregar miembro, quitar miembro, obtener asociación
- Información: ping, obtener información, solicitar una devolución de la llamada en la ocurrencia de un evento

2.2.5 Protocolo de descubrimiento del servicio SDP

2.2.5.1 Descripción

El mecanismo de descubrimiento del servicio proporciona los medios a las aplicaciones clientes para descubrir la existencia de servicios proporcionados por aplicaciones servidor así como también los atributos de esos servicios. Los atributos de un servicio incluyen el tipo o la clase del servicio ofrecido y la información de mecanismo o protocolo necesitado para utilizarlo (figura 16)

Figura 16. Esquema SDP



SDP es un protocolo sencillo con requisitos mínimos de transporte. Puede funcionar sobre transporte seguro de paquetes (o incluso no seguro si el cliente implementan timeouts y peticiones de repetición si es necesario). SDP utiliza un modelo petición/respuesta donde cada transacción se compone de una unidad de datos (PDU) del protocolo de petición y una PDU respuesta. Sin embargo, los pedidos se pueden encaminar potencialmente y las respuestas se pueden devolver potencialmente fuera de orden.

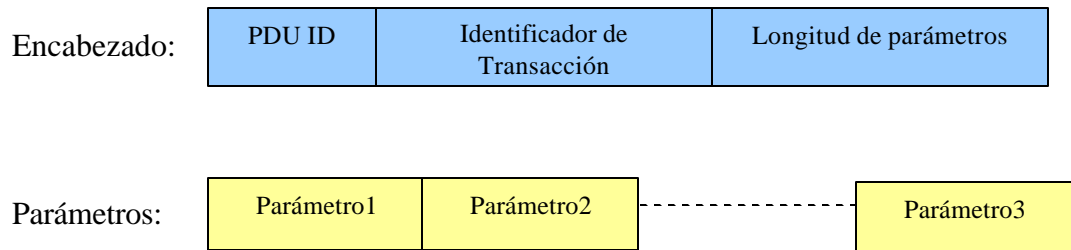
En el caso específico donde SDP utiliza el protocolo del transporte de Bluetooth L2CAP, múltiples PDUs SDP se pueden mandar en un solo paquete L2CAP, pero sólo puede haber un paquete L2CAP por conexión a un servidor determinado en un instante dado. En otras palabras un cliente solo puede recibir una respuesta a cada pedido antes de enviar otra petición en la misma conexión L2CAP. Limitando al SDP a mandar un paquete de no reconocimiento se ofrece una forma simplificada de control de flujo.

2.2.5.2 Formato de PDU

Cada PDU consta de un encabezado de PDU seguido por parámetros específicos de PDU. El encabezado consta de tres campos: Un identificador de PDU (ID PDU), un identificador de transacción que sólo identifica PDUs de petición y se usa para igualar las PDU de respuesta a las PDUs de petición y un campo de

longitud de parámetro que especifica la longitud de todos los parámetros contenidos en la PDU (figura 17).

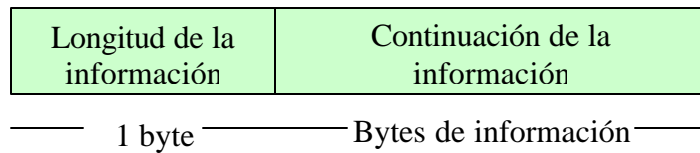
Figura 17. Formato de las PDU



2.2.5.3 Respuestas parciales y estado de la continuación

Algunas peticiones 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 proporcionado por el cliente en la petición siguiente para recuperar la próxima porción de la respuesta completa. El parámetro del estado de continuación es un campo de longitud variable cuyo primer byte contiene el número de bytes adicionales de información de continuación en el campo. El formato de la información de continuación no se estandariza entre servidores SDP. Cada parámetro del estado de continuación es significativo sólo para el servidor SDP que lo generó (figura 18).

Figura 18. Formato del estado de continuación



2.2.5.4 Manejo de errores

Si el servidor determina que una petición se ha realizado de forma inapropiada o por alguna razón el servidor no puede responder con el tipo apropiado de PDU, responderá con una PDU de error.

2.2.5.5 Servicios SDP

En este aparte se describe cómo se almacenan las características (servicios) individuales de los distintos dispositivos Bluetooth.

2.2.5.5.1 Registro del Servicio

Un servicio es cualquier entidad que puede proporcionar información, realizar una acción, o controlar un recurso a favor de otra entidad. Un servicio se puede implementar como software, hardware, o una combinación de hardware y software. Toda la información acerca de un servicio que mantiene un servidor de SDP está contenida dentro de un solo registro del servicio. El registro del servicio consiste básicamente de una lista de atributos del servicio.

2.2.5.5.2 Atributos del servicio

Cada atributo del servicio describe una sola característica de un servicio. Un atributo del servicio se compone de dos partes:

- **Una identificación del atributo:** Es un entero sin signo de 16 bits que distingue cada atributo del servicio de otros atributos del servicio dentro de un registro del servicio.
- **El valor del atributo:** Es un campo de longitud variable cuyo significado es determinado por la identificación del atributo asociada a él y por la clase de servicio del registro del servicio en que el atributo está contenido.

2.2.5.5.3 Clase de servicio

Los servicios se agrupan formando clases de servicio. Un registro del servicio contiene los atributos que son específicos a una clase del servicio así como también los atributos universales que son comunes a todos los servicios. Cada definición del atributo especifica el valor numérico de la identificación del atributo, el uso destinado del valor del atributo, y el formato del valor del atributo.

A cada clase del servicio se le asigna una identificación única, un UUID, que es un valor de 128 bits. Un UUID es una identificación universalmente única garantizada a través de todo espacio y todo el tiempo. Las UUIDs se puede crear independientemente de manera distribuida, y no se requiere un registro central de UUIDs.

2.2.5.5.4 Descubrimiento del servicio

El propósito de SDP es permitir a los dispositivos Bluetooth descubrir los servicios que otros dispositivos de la misma tecnología pueden ofrecer. SDP permite esto de varias formas: Modo de búsqueda (Searching) el cual busca el servicio específico, y el Modo Navegador (Browser) que verifica qué servicios se ofrecen verdaderamente.

2.2.6 Interfaz controladora de host (HCI)

El HCI es un interfaz que envía órdenes al controlador de Banda Base y al Administrador del Enlace (LM, Link Manager), y proporciona acceso al estado del hardware y a los registros de control. Esencialmente este interfaz proporciona un método uniforme de acceso a las capacidades de Banda Base de Bluetooth. El HCI actúa a través de tres secciones, Host - Capa de Transporte - Controlador de

Host. Cada una de las secciones tiene una función diferente que desempeñar en el sistema de HCI.

2.2.6.1 Componentes principales HCI

El HCI se divide funcionalmente en 3 bloques:

- El *Firmware* que se localiza en el Controlador de Host y se encarga de implementar las ordenes de HCI para el hardware Bluetooth, accediendo a órdenes de la Banda Base, del administrador de enlace (LM), a los registros de control y de eventos. El controlador de host es el que habilita al HCI en los dispositivos Bluetooth.
- El *Driver* HCI que se localiza en el host y es el que recibe las notificaciones de los eventos asíncronos del HCI bs cuales notifican al host la ocurrencia de algún evento. Cuando el host verifica lo anterior envía un análisis del paquete del evento recibido para determinar cuál de todos los posibles eventos fue el que ocurrió.
- Los dos elementos anteriormente mencionados se comunican a través de la *Capa de Transporte del Controlador de Host*, es decir que son varias capas que pueden existir entre el driver de HCI en el sistema del Host y el Firmware

de HCI en el hardware de Bluetooth. Estas capas intermedias deben posibilitar la transferencia de datos sin el conocimiento interno de los datos para se transfieren. Pueden usarse varias capas diferentes del Controlador de Host, de las cuales 3 han sido definidas inicialmente para Bluetooth: USB, UART y RS232. El Host debe recibir las notificaciones de eventos asíncronos de HCI independientemente de qué Capa de Transporte de Controlador de Host se utiliza.

2.2.6.2 Comandos HCI

HCI proporciona un método uniforme de comandos para acceder a las capacidades del hardware Bluetooth. Estos comandos pueden tomar distintos intervalos de tiempo para completarse, razón por la cual los resultados son reportados al Host en forma de eventos. En la tabla 6 se explican las funciones de los principales comandos de las capas HCI.

COMANDO	DESCRIPCION
Intercambio de información HCI específica	La Capa de Transporte del Controlador de Host proporciona el intercambio transparente de información HCI específica. Este mecanismo de transporte proporciona al host la capacidad para el envío de comandos, paquetes ACL y SCO al controlador de host y viceversa.
Control de enlace	Los comandos del Control de Enlace permiten al Controlador de Host administrar las conexiones hacia otros dispositivos Bluetooth. Cuando se utilizan estos comandos, el Administrador de Enlace controla la forma en que se establecen y mantienen las Piconets y Scatternets.
Políticas de Enlace	Estos comandos proporcionan métodos para que el host afecte la forma como el Administrador de Enlace (LM) maneja la piconet. Cuando se utilizan los comandos de políticas, el LM controla todavía la forma en que se establecen y mantienen las piconets y scatternets de Bluetooth, dependiendo de los parámetros ajustables de la política; modifican el comportamiento del LM y puede tener como resultado cambios en las conexiones de la capa del enlace de dispositivos remotos.
Controlador de Host y Banda Base	Estos comandos proporcionan control de los dispositivos Bluetooth y de las capacidades del Controlador de Host, Administrador de Enlace y Banda Base. El dispositivo host puede utilizarlos para modificar el comportamiento de un dispositivo local.
Parámetros de información	Estos parámetros son fijados por el fabricante del dispositivo Bluetooth. Proporcionan información sobre el dispositivo y sobre las capacidades del Controlador del Host, del Administrador de Enlace y de la Banda Base. No pueden ser modificados por el por el dispositivo host.
Parámetros de estado	El Controlador del Host modifica todos estos parámetros, los cuales brindan información del estado actual del Controlador del Host, del Administrador de Enlace y de la Banda Base. El dispositivo host no puede modificar estos parámetros excepto colocar algunos parámetros específicos a cero.

Tabla 6. Comandos HCI

2.2.6.3 Eventos HCI, Códigos de Error y Control de Flujo

Los eventos HCI proveen un método para devolver parámetros y datos asociados con cada evento, tales como errores de hardware, cambios de rol, conexiones y desconexiones, búsqueda entre otros.

Cuando un comando falla, el dispositivo envía de vuelta un *código de error* indicando la razón de ésta. Hasta el momento hay definidos 35 de estos códigos como los fallos de hardware, memoria llena, superación de tiempo de espera en una conexión, comandos HCI no reconocidos, etc.

En cuanto al *control de flujo*, es utilizado en la dirección Host-Controlador de Host para evitar el llenado de los registros de datos de este último con datos ACL destinados para un dispositivo remoto que no responde. El host es el que se encarga de la administración de los registros de datos del Controlador de Host.

2.2.7 Protocolo de reemplazamiento de cables RFCOMM

RFCOMM es un protocolo simple de transporte proveído de funciones adicionales que emula los nueve circuitos del puerto serial RS232. La emulación de los puertos serie la hace sobre L2CAP y se basa en el estándar ETSI TS 07.10. Este protocolo soporta hasta 60 conexiones simultáneas entre dos dispositivos

Bluetooth. Estas conexiones dependen de la implementación específica que se utilice.

2.2.7.1 Tipos de dispositivos

Para propósitos del protocolo RFCOMM, una comunicación completa incluye dos aplicaciones ejecutándose en dispositivos diferentes con un segmento de comunicaciones entre ellos. Son dos las clases de dispositivos:

- **Tipo 1:** Son puntos finales de comunicación tales como impresoras o PC's.
- **Tipo2:** Son aquellos que forman parte del segmento de comunicación. Como por ejemplo un MODEM.

2.2.7.2 Emulación de múltiples puertos seriales

Dos dispositivos Bluetooth utilizando en su comunicación RFCOMM, pueden abrir varios puertos seriales emulados. Un DLCI (Identificación de Conexión de Enlace de Datos) identifica una conexión de una aplicación entre cliente y servidor. El DLCI se representa por 6 bits, pero su rango utilizable es de 2 a 61. El DLCI es único dentro de una sesión de RFCOMM entre dos dispositivos.

Para dar cuenta del hecho de que las aplicaciones de cliente y servidor pueden residir en ambos lados de una sesión de RFCOMM, con clientes en cualquier lado haciendo conexiones independientes de los demás, el espacio de valor del DLCI se divide entre los dos aparatos que se comunican usando el concepto de canales de servidor de RFCOMM.

Si un dispositivo Bluetooth mantiene varios puertos seriales emulados y se permite que las conexiones tengan puntos finales en dispositivos diferentes de Bluetooth, entonces la entidad de RFCOMM debe ser capaz de hacer funcionar múltiples sesiones TS 07.10 multiplexadas. Hay que tener en cuenta que cada sesión multiplexada usa su propia identificación de canal L2CAP (CID). La facultad de hacer funcionar múltiples sesiones de TS 07.10 es opcional para RFCOMM.

2.2.8 Protocolo de Control de Telefonía Binario

El protocolo de Control de Telefonía Binario (TCS Binario o TCS BIN), define la señalización de control para el establecimiento de una conversación y para llamadas de datos entre dos dispositivos Bluetooth. Además, define un procedimiento de gestión de la movilidad para manejar grupos de dispositivos Bluetooth TCS. TCS Binario viene definido en la especificación del Protocolo de

Control de Telefonía de Bluetooth, y está basado en la recomendación ITU-T Q.931. El TCS contiene las siguientes funcionalidades:

- Control de Llamada (CC): Maneja las señales para el establecimiento y desconexión de las llamadas de voz y datos entre dispositivos Bluetooth.
- Manejo de grupos: señalización para el fácil manejo de grupos de dispositivos Bluetooth.
- TCS no orientado a conexión (CL): Proporciona el intercambio de información no relacionada con las llamadas en progreso.

2.2.9 Protocolos Adoptados

2.2.9.1 PPP

En la tecnología Bluetooth PPP está diseñado para funcionar sobre RFCOMM y establecer conexiones punto a punto. PPP es el protocolo punto a punto de IETF y su misión es tomar paquetes IP desde o hacia la capa PPP y colocarlos en la LAN.

2.2.9.2 TCP/UDP/IP

Son protocolos definidos por el IETF y se utiliza para las comunicaciones a través de Internet. Son considerados como la familia de protocolos mas usada en el mundo y la pila TCP/IP se encuentra presente en numerosos dispositivos como PC's, impresoras, PDA's entre otros. La implementación de estos estándares en dispositivos Bluetooth permite la comunicación con cualquier otro dispositivo que esté conectado a Internet. Por ejemplo, un headset o un punto de acceso de datos, se utilizará como bridge a Internet.

2.2.9.3 Protocolo OBEX

IrOBEX, o de forma mas sencilla OBEX, es un es un protocolo de sesión desarrollado por la Asociación de Datos Infrarrojos (IrDA) para intercambiar objetos de forma simple y espontánea. OBEX, que ofrece la misma base funcional que HTTP pero de una forma más ligera, utiliza un modelo cliente-servidor y es independiente del mecanismo de transporte y el API (Access Point Interface) de transporte, ofreciendo así una base de transporte fiable. OBEX ofrece también un modelo de representación para objetos y operaciones para comunicarse con otros dispositivos. Además, el protocolo OBEX permite navegar por los contenidos de las carpetas de un aparato remoto.

En una primera fase, RFCOMM se usa como la única capa de transporte para OBEX. Implementaciones futuras prometen ofrecer también transporte TCP/IP.

2.2.9.3.1 Formato de contenidos

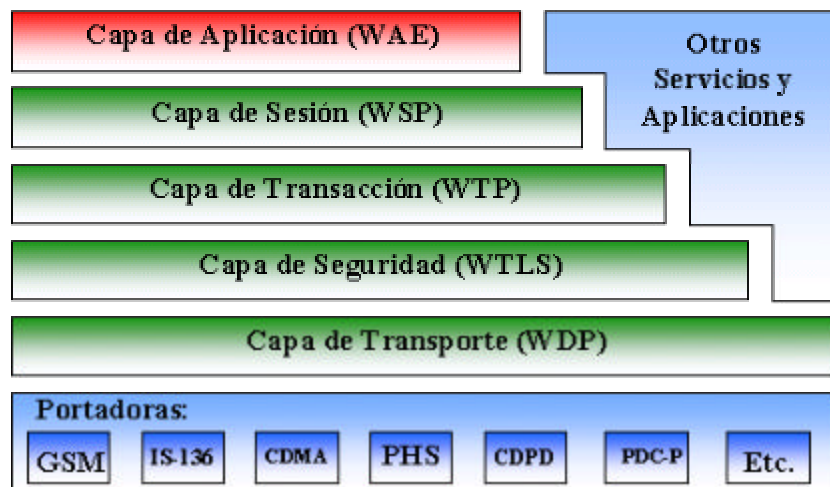
vCard y vCalendar son especificaciones abiertas controladas ahora por el Consorcio de Correo de Internet. Estas especificaciones definen el formato de una tarjeta de negocios electrónica y de entradas de información personal en el calendario, respectivamente. vCard y vCalendar no definen ningún mecanismo de transporte sino sólo el formato bajo el cual se transportan los datos. Adoptando vCard y vCalendar, el SIG ayuda a impulsar más el intercambio de información bajo estos formatos bien definidos que se ofrecen. Las especificaciones vCard y vCalendar están accesibles desde el Consorcio de Correo de Internet y están siendo más desarrolladas por el IETF.

Otros formatos de contenidos, que se transfieren por el OBEX en Bluetooth, son vMessage y vNote. Estos formatos de contenidos también son estándares abiertos y se usan para intercambiar mensajes y notas. Vienen definidos en la especificación IrMC, que también define un formato para los archivos fragmentados que necesitan sincronización de datos entre dispositivos

2.2.9.4 WAP

Los modelos para funciones como por ejemplo control remoto, búsqueda de datos desde un PC hacia un handset, etc, pueden ser implementados utilizando las características de WAP. El Foro del Protocolo de Aplicación Inalámbrico (WAP) está preparando una especificación de protocolo inalámbrico, que trabaja a través de varias tecnologías de redes inalámbricas de área amplia. La meta es aportar contenidos de Internet y servicios de telefonía a teléfonos móviles celulares y otros terminales inalámbricos. La figura 19 representa la pila de protocolos del sistema WAP.

Figura 19. Protocolo WAP



La idea detrás de la elección de WAP es reutilizar las aplicaciones software desarrolladas por el Entorno de Aplicación de WAP. Estas incluyen los navegadores WML y WTA que pueden interactuar con aplicaciones de PC.

3. IMPLEMENTACION

El costo de implementar esta tecnología es significativamente alto aunque está con tendencia a la baja por la cantidad de productos que se lanzan al mercado por parte de diversas empresas. A continuación se referencian algunos de los elementos necesarios para poder poner en marcha una pequeña sala con tecnología Bluetooth en la Tecnológica de Bolívar y así poder determinar cuales son las ventajas y desventajas en el uso de éstos:

	ADAPTADOR USB TECOM \$131.000	El adaptador USB Bluetooth TECOM BT-3034 proporciona a cualquier computador portátil o de escritorio, conectividad inalámbrica mediante tecnología Bluetooth de una manera sencilla y rápida. Dispone de instaladores y software de control para sistema operativo Windows,98,Me, 2000 y XP.
	ADAPTADOR IMPRESORA BLUETAKE BT200 \$402.000	El adaptador Bluetooth para impresoras BT200 de BlueTake, se conecta directamente a cualquier impresora con conector paralelo y permite imprimir de una manera fácil y rápida desde un ordenador portátil, PDA, Teléfono móvil o cualquier otro dispositivo portatil con tecnología Bluetooth desde una distancia de 10 a 100 metros
	ACCESS POINT LAN TECOM BT3021 \$352.000	El BT3021 de TECOM es un punto de acceso inalámbrico Bluetooth con conexión Ethernet que permite acceder de forma remota a los contenidos de Internet o a la red Corporativa, ya sea desde un PC, PDA, o teléfono móvil equipados con Bluetooth, de una manera simple, sencilla y totalmente inalámbrica.

4. APLICACIONES

El Bluetooth SIG y sus compañías patrocinantes han propuesto diversas soluciones e implementado una buena cantidad de escenarios de prueba entre los cuales se encuentran los siguientes:

- **Automatización Hotelera:** la cadena de hoteles Holiday Inn, Axis Communications AB y Registry Magic han juntado sus esfuerzos para convertir el Holiday Inn de Wall Street en el primer hotel en prestar servicios inalámbricos. La tecnología permitirá a los huéspedes hacer su "check-in" y "check-out", entrar a sus habitaciones, utilizar Internet, recibir mensajes de voz, y pagar comidas en el restaurante del hotel.

Paralelamente, hay iniciativas como la de la compañía **i-Wap** para simplificar tareas de la administración hotelera, como por ejemplo el monitoreo de consumo de mini-bar, y el manejo de órdenes de "Room-Service".

- **Acceso a Internet en aeropuertos:** muchos ejecutivos que viajan regularmente se ven cada vez más en necesidad de tener acceso continuo

a su correo electrónico y al Web. Hasta ahora la solución adoptada por muchos suele ser una llamada telefónica a un número de acceso de su proveedor o una complicada y costosa conexión a través de un teléfono celular. Actualmente, compañías como American Airlines y TWA están implementando el servicio de Internet Inalámbrico en sus salas de espera de primera clase. A pesar de los esfuerzos de ambas compañías, han encontrado un gran número de obstáculos para la implantación del servicio. El hecho que principalmente ha retardado la implantación de Bluetooth dentro de ésta área es que se trata de una tecnología en vías de desarrollo. Adicionalmente las operadoras de los aeropuertos y las compañías de telefonía de larga distancia, al ver sus intereses en peligro, han comenzado a dificultar deliberadamente la entrada de las WPANs en las instalaciones de los aeropuertos.

- **Acceso a información en trenes:** BT Syncordia y Midland Mainline han comenzado pruebas para verificar la factibilidad de utilizar intranets basados en Bluetooth dentro de sus vagones. Dentro de los trenes, los usuarios tendrán acceso a ciertas páginas Web de noticias obtenidas con antelación y almacenadas en un "Cache" del tren. Posiblemente se contempla la posibilidad de que los pasajeros adquieran sus tickets a través de este medio. Una conexión "en vivo" en los trenes haría mucho más interesante la implantación de ésta propuesta.

CONCLUSIONES

Las desventajas y ventajas de esta tecnología vienen dadas por su naturaleza inalámbrica y el manifiesto deseo de los fundadores de conseguir unos precios para sus chips lo suficientemente económicos como para poder integrarse con diversos dispositivos. El mercado global es quien determinará en que medida la estructura de su protocolo y el uso de frecuencias permitan su sobrevivencia, ya que en la actualidad existen tecnologías que utilizan frecuencias similares como lo son la WLAN o WIFI que dentro del mercado de las redes tienen una buena aceptación de los consumidores ya que haciendo uso de este ethernet inalámbrico, permite establecer redes de PC's y periféricos sin utilizar cables y sin limitaciones de dispositivos en la red y con mayores distancias.

Comparada con la tecnología Wi-Fi, Bluetooth tiene menos posibilidades de alcanzar un mayor cubrimiento en el mercado ya que Wi-Fi ofrece un mayor rango de alcance y mejores velocidades de acceso. También está el tema precios, en el cual Wi-Fi lleva la delantera por tener mayor aceptación en el mercado y contar con variedad de productos que satisfacen las necesidades de cada usuario. Otro punto a favor es la puesta en marcha de los famosos puntos de acceso inalámbricos personales, que consiste en que los moradores de varias viviendas montan puntos de acceso Wi-Fi para compartir la conexión a Internet.

En cuanto a la capacidad para poder soportar aplicaciones de gruesa envergadura, Bluetooth presenta un pobre desempeño y quedó demostrado en una prueba que hicieron en un congreso de proveedores de esta tecnología en la cual se trató de descargar un archivo de 700 Kb por Internet a través de una PDA y el tiempo de bajada dejó mucho que desear. Ahora si tuviéramos los 8 dispositivos que soporta una piconet tratando de utilizar este servicio veríamos que no sería la mejor elección de tecnología para suplir las necesidades de una red. Hasta el momento está quedando demostrado que Bluetooth solo sirve para implementar una red casera en la cual tengamos que enviar mensajes de texto, imprimir páginas, bajar archivos pequeños desde Internet, actualizar nuestra libreta de direcciones entre la PDA y nuestro portátil o desktop, etc.

Si las compañías quisieran mejorar la velocidad de transmisión y la cobertura del rango de radio frecuencia, la tecnología se vería en serios problemas ya que tendrían que aumentar el tamaño del chip para poder tener más potencia y por ende el precio de los dispositivos se irían por las nubes quedando de esta manera menos asequible para su implementación en entornos caseros y/o organizacionales.

Es así como la lucha del SIG por mejorar el funcionamiento de Bluetooth para seguir teniendo aceptación entre los asiduos a esta tecnología, determinará su continuidad o desaparición del mundo de las redes inalámbricas.

GLOSARIO

PAN (Personal Area Network): interconexión de dispositivos de información dentro de un rango de acción de una persona, que típicamente es de 10 metros.

WPAN: red de área personal inalámbrica.

AD-HOC: redes que se forman a través de conexiones instantáneas. Son redes que no necesitan de una planeación previa.

ITU: Unión Internacional de Telecomunicaciones, la cual coordina los servicios y redes mundiales de telecomunicaciones.

LAN (Local Area Network): red de área local.

WAN (Wide Area Network): red de área extendida.

MODULACIÓN: técnicas para el transporte de información sobre una onda portadora.

PROTOCOLO: conjunto de normas que determinan la manera en que se realiza el intercambio de información en una red.

CSVD (Modulación Delta Continua con Pendiente Variable): método de modulación utilizado para la transmisión de voz.

IETF (Internet Engineering Task Force): Grupo de Tareas sobre Ingeniería de Internet.

PUNTO DE ACCESO: dispositivo que se encarga de transportar información entre una red cableada y una inalámbrica.

FRECUENCIA: La frecuencia es el número de oscilaciones por unidad de tiempo que tiene una onda electromagnética.

DISPOSITIVO MAESTRO: dispositivo con la tecnología Bluetooth que se encarga de la administración de una piconet al sincronizar a los esclavos a su reloj y frecuencia.

BIBLIOGRAFIA

MSI PC2PC™-- Bluetooth [on line]. Disponible desde internet:

<http://www.msiami.com/NEW/spanish/noticias/Bluetooth.htm>

Las redes personales [online]. Revista PC World. Angélica Gómez. Septiembre 12 del 2003. Disponible desde Internet:

<http://www.pcworld.com.ve/n54/articulos/informe3.html>

Bluetooth, comunicación sin hilos [on line]. Disponible desde Internet:

<http://www.tiramillas.net/videojuegos/guiautil/bluetooth/xircom.html>

Comienza el boom del Internet inalámbrico [on line]. Evelio Martínez. Enero del 2001. Disponible desde Internet:

http://eveliux.com/articulos/internet_inal.html

Bluetooth Tutorial [on line]. Disponible desde Internet:

<http://www.palowireless.com/infotooth/tutorial>

Personal Area Networks: Near-field intrabody communication [on line]. Thomas G. Zimmerman. Abril 8 de 1996. Disponible desde Internet:

<http://www.research.ibm.com/journal/sj/353/sectione/zimmerman.html>

PAN (Personal Area Network) [on line]. Disponible desde Internet:

<http://www.nwfusion.com/links/Encyclopedia/P/468.html>

Personal Area Network [on line]. Nitesh Ambastha. Abril del 2000. Disponible desde Internet:

<http://www.acm.org/chapters/bombay/news/articles/20000401.html>

Personal Area Network, A Bluetooth Primer [on line]. Albert Proust. Marzo 11 del 2003. Disponible desde Internet:

<http://www.oreillynet.com/pub/a/wireless/2000/11/03/bluetooth.html>

Building a Home Office Network [on line]. Peter Ruber. Junio 15 del 2001. Disponible desde Internet:

<http://www.internetworld.com/magazine.php?inc=061501/06.15.01feature5.html>

Personal Area Networks - A Review of the Technology and Possible Applications [on line]. Heath Conn and Bob Nerenberg. University of Washington. Disponible desde Internet:

<http://faculty.washington.edu/sandeep/future/PAN.doc>

¿Qué es Bluetooth? [on line]. Albert García. Disponible desde Internet:

http://www.zonablueetooth.com/que_es_bluetooth.htm

Bluetooth Core Specifications [on line]. Disponible desde Internet:

<http://www.bluetooth.com>