

Capítulo 3

Bluetooth como tecnología inalámbrica

La tecnología inalámbrica Bluetooth se ha convertido en una especificación global como mecanismo para establecer una comunicación rápida, fiable y sin cables entre multitud de dispositivos como pueden ser ordenadores portátiles, teléfonos móviles, periféricos o manos libres para vehículos motorizados. El principal motivo de su rápida extensión se debe a la facilidad para transferir datos y sincronizar dispositivos. No obstante, en el ámbito industrial esta tecnología ha despertado un creciente interés como consecuencia de su bajo coste y gran capacidad de transmisión, además de su rápida implantación en la mayor parte de los dispositivos móviles multimedia comerciales.

En el resto del capítulo se analizarán las principales características del estándar en su versión 2.1, de forma que se pueda obtener una visión general del mismo y se detallarán aquellos conceptos claves para el desarrollo de este proyecto.

3.1. Descripción general

Bluetooth surge como una especificación para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre (2,4 GHz.). Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

En 1994, Ericsson inició un estudio para investigar la viabilidad de una nueva interfaz de bajo costo y consumo para la interconexión vía radio (eliminando así cables) entre dispositivos como teléfonos móviles y otros accesorios. El estudio partía de un largo proyecto que investigaba 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 haciendo claro que éste tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenía como principal virtud que se basaba en un chip de radio.

De esta forma, se creó el protocolo de comunicaciones inalámbricas Bluetooth cuyas distintas versiones son:

- Bluetooth v.1.1 (IEEE Standard 802.15.1-2002)
- Bluetooth v.1.2 (IEEE Standard 802.15.1-2005)
- Bluetooth v.2.0 (Bluetooth 2.0 + EDR publicada por el SIG)
- Bluetooth v.2.1 +EDR(Bluetooth Core Specification Version 2.1 publicada por el SIG el 26 de Julio de 2007)
- Bluetooth v.3.0 +HS(Abril de 2009)

La versión 1.2, a diferencia de la 1.1, adopta una solución inalámbrica complementaria para permitir la coexistencia de sistemas Bluetooth y Wi-Fi en el espectro de los 2.4 GHz, sin interferencia entre ellos. Para ello, usa la técnica de saltos en frecuencias adaptativos (AFH), que consigue una transmisión más eficiente y un cifrado más seguro. Para mejorar las experiencias de los usuarios, esta versión ofrece una calidad de voz con menor ruido ambiental, y permite una rápida configuración de la comunicación con otros dispositivos Bluetooth dentro del rango del alcance.

La versión 2.0, fue creada para ser una especificación separada. Se caracteriza por incorporar la técnica "Enhanced Data Rate" (EDR) que le permite mejorar las velocidades de transmisión en hasta 3Mbps a la vez que intenta solucionar algunos errores de la especificación 1.2.

La versión 2.1, simplifica los pasos para crear la conexión entre dispositivos, además el consumo de potencia es 5 veces menor. No obstante, se han añadido otras mejoras sustanciales a la especificación como la generación de informes de datos erróneos, la respuesta extendida al proceso de descubrimiento, eventos de finalización por extinción del temporizador en la supervisión del enlace o el modo de seguridad 4.

Finalmente, la versión 3.0 añade nuevas mejoras al estándar Bluetooth en relación a la pila de protocolos usada. Se introdujo la capa AMP, lo que ha provocado una mejora de la capa HCI para interactuar con AMP de una forma más óptima así como la seguridad. Se ha mejorado el protocolo L2CAP con la inclusión de los modos Streaming y de retransmisión mejorada, se han solucionado problemas en el soporte del canal así como una mejora de la máquina de estados L2CAP para los canales AMP. Como una característica novedosa, se encuentra una capa de adaptación del protocolo 802.11.

En relación a los aspectos más tecnológicos, la tecnología inalámbrica Bluetooth utiliza la banda de radio ISM (Industrial, Science and Medical applications) de 2,4 GHz. que se encuentra disponible en todo el mundo y que no requiere de una licencia por parte de las autoridades reguladoras de las telecomunicaciones propias de cada país. Esto permite que los dispositivos Bluetooth puedan operar en cualquier región del globo terrestre sin necesidad de cambiar ningún componente hardware del dispositivo.

El sistema emplea un transmisor de salto en frecuencia para contrarrestar las interferencias y las pérdidas de intensidad de señal, y cuenta con un gran número de portadoras disponibles para la transmisión de datos debido al uso de una modulación espectro ensanchado por salto en frecuencia (FHSS). Para minimizar la complejidad del transmisor, se utiliza una modulación de frecuencia binaria. La tasa de transferencia de símbolos es de 1M Símbolo/s, admitiendo una velocidad de hasta 1 Mbps en el modo de transferencia básica y una velocidad de transmisión aérea total de 2 a 3 Mbps en el modo de transferencia mejorada o EDR. Este último modo se corresponde con una especificación incluida en la especificación 2.1 del estándar Bluetooth.

Por su parte, sobre esta interfaz radio, se definen dos tipos de enlaces: físicos y lógicos. Los enlaces físicos se corresponde con un enlace de comunicación entre dos dispositivos que se intercambian paquetes, sea cual sea la dirección de estos. No obstante, la norma impide que todos los dispositivos puedan establecer enlaces con todos, sino que sólo podrán establecer un enlace físico dentro de una misma red el maestro y un esclavo. De forma que dos dispositivos que actúen como esclavos en una red no podrán formar un enlace físico nunca.

Con respecto a los enlaces lógicos, estos son los que permiten soportar las aplicaciones de voz y datos. Estos se corresponden con enlaces SCO y con enlaces ACL, respectivamente. Los enlaces ACL, se tratan de enlaces asíncronos no orientados a conexión, por lo que

proporcionan un enlace no fiable de tal forma que los paquetes que se envían a través de estos enlaces no se garantizan que se entreguen al otro extremo del enlace. Por esta razón este tipo de enlaces son convenientes para servicios basados en conmutación de paquetes. En relación a los enlaces SCO, su principal característica es que se corresponden con enlaces síncronos orientados a conexión, por lo que han sido diseñados para soportar voz en tiempo real y tráfico multimedia. Por ello, son ideales para servicios que requieran un enlace fiable de transmisión o estén basados en conmutación de circuitos. Tanto la voz como los datos se transmiten en forma de paquetes y la especificación Bluetooth permite crear enlaces ACL y SCO al mismo tiempo.

Finalmente, la pila de protocolos que usa Bluetooth se organiza en capas al igual que el modelo OSI. En la figura 3.1.1 se pueden comprobar los diferentes protocolos de los que hace uso la especificación para gestionar y controlar los diferentes enlaces y conexiones. Cada uno de estos protocolos será revisado en secciones posteriores del capítulo.

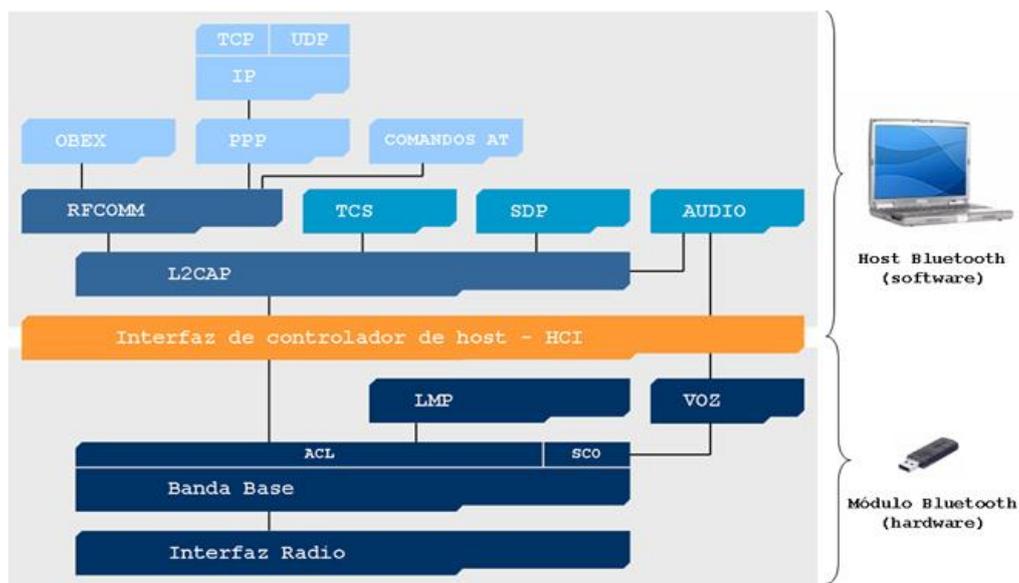


Figura 3.1.1. Pila de protocolos Bluetooth.

3.2. Arquitectura Bluetooth

La pila de protocolos Bluetooth se basa en el modelo de referencia OSI del organismo internacional de estandarización ISO para la interconexión de sistemas abiertos. La especificación Bluetooth utiliza una arquitectura de protocolos que permiten el intercambio transparente de datos entre aplicaciones diseñadas de acuerdo con dicha especificación y fomentan la interoperabilidad entre los productos de diferentes fabricantes.

Se pueden observar dos áreas en dicha pila de protocolos, que pueden ser implementadas en distintos sistemas o todos en un mismo sistema. Estas áreas son:

- **El módulo Bluetooth (periférico hardware)**, encargado de las tareas relacionadas con el envío de información a través de la interfaz de radiofrecuencia. Se encargaría de las tareas asignadas a la capa física y parte de la capa de enlace en el modelo OSI. Esto supone la codificación de los bits, la modulación utilizada o la potencia con la que se transmite.
- **El host Bluetooth (implementación software)**, relacionado con los protocolos asociados a las capas superiores como la capa de red o de aplicación.

El nexo de unión entre estas dos zonas diferenciadas es la denominada Interfaz de Controlador de Host o, por sus siglas en inglés, HCI. Se encarga de suministrar una interfaz uniforme de acceso a las capacidades del controlador Bluetooth a través de un conjunto de comandos que afectan a diferentes bloques de la arquitectura de Bluetooth como puede ser el gestor de enlaces o la banda base.

En las siguientes subsecciones se procederá a detallar el funcionamiento básico de los bloques que componen la especificación Bluetooth.

3.2.1. Radio

Como se ha comentado anteriormente, los dispositivos Bluetooth operan sobre la banda ISM de 2.4 GHz. utilizando un transceptor de salto en frecuencias para combatir las interferencias y los desvanecimientos en la señal causados por el medio físico. En concreto, las frecuencias operativas de Bluetooth se hallan mediante la expresión 3.1:

$$f_k = 2402 \text{ (MHz)} + k \text{ con } k = 0,1, \dots,78$$

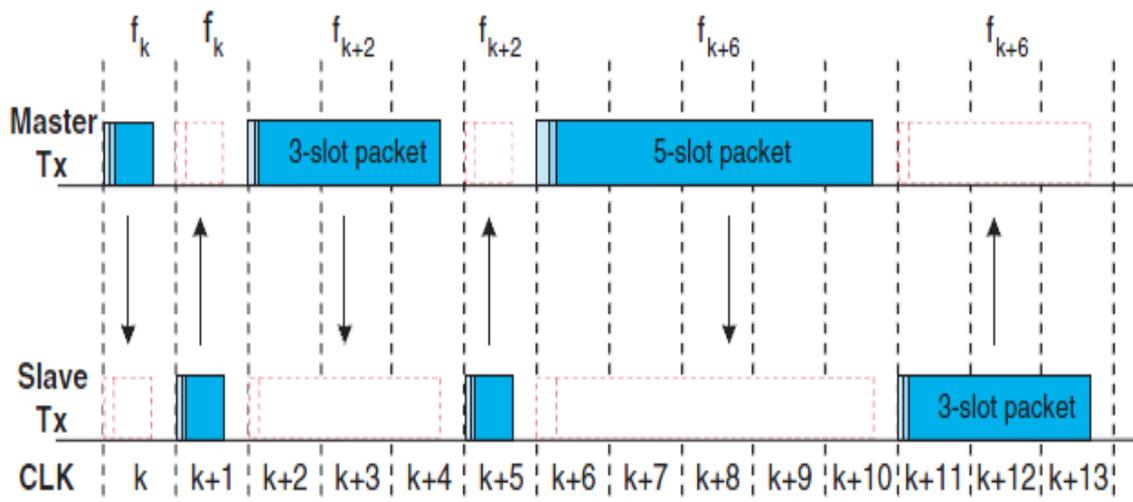
Ecuación 3.2.1. Expresión que permite hallar las frecuencias centrales de los canales Bluetooth.

Como se puede comprobar del análisis de la expresión 3.2.1, los canales de radiofrecuencia están espaciados 1 MHz en el espectro. Además para cumplir con las regulaciones fuera de banda de cada país, se ha dejado una banda de guardia de 2 MHz en el límite inferior de la banda y de 3.5 MHz en el superior.

Por su parte, la especificación define dos tipos de modulaciones dependiendo la usada para transmitir del modo de operación del dispositivo. De esta forma, si se operan en el modo

normal denominado Basic Rate y que alcanza una velocidad de transmisión máxima de 1 Mbps, se usa una modulación FM binaria que minimiza la complejidad del transceptor. No obstante, se define un modo opcional de transmisión que permite alcanzar una mayor velocidad de transmisión, denominado Enhanced Data Rate, que usa una modulación PSK y que posee dos variantes a su vez: $\frac{\pi}{4}$ -DQPSK, que permite alcanzar los 2 Mbps, y 8DPSK, con la que se pueden obtener hasta 3 Mbps de tasa de bits. La tasa de símbolos para ambas modulaciones es de 1 MSímbolo/s.

Para poder efectuar una transmisión full-duplex, se ha optado por usar un esquema de multiplexación por división en el tiempo (TDD) en ambos modos. Este mecanismo permite emular un canal de comunicación full dúplex a partir de un enlace de comunicaciones semi-duplex. Para ello, lo que se hace es dividir el tiempo en ranuras o slots, asignando un cierto número de ellos al enlace de subida y otros al enlace de bajada. Esto supone una gran ventaja cuando los enlaces son asimétricos ya que permiten asignar más capacidad al canal que lo requiera.



Ecuación 3.2.2. Ejemplo de un esquema de multiplexación por división en el tiempo en una comunicación Bluetooth.

El otro aspecto más importante de la interfaz radio se corresponde con la potencia de transmisión. Según la potencia máxima de salida, en la especificación Bluetooth se distinguen tres tipos de dispositivos:

Clase	Potencia máxima de salida (Pmax)	Potencia Nominal	Potencia mínima de salida (Pmin)	Control de potencia	Alcance
-------	----------------------------------	------------------	----------------------------------	---------------------	---------

1	100 mW (20 dBm)	N/D	1 mW (0 dBm)	0	Pmin < +4 dBm a Pmax	~100 m
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	0	Opcional: Pmin ² a Pmax	~10 m
3	1 mW (0 dBm)	N/D	N/D	0	Opcional: Pmin ² a Pmax	~1 m

Tabla 3.2.1. Especificación de las clases de dispositivos y sus características.

La clase de dispositivo Bluetooth es un parámetro importante a la hora de usarlo en una aplicación ya que determinará el alcance máximo del sistema.

3.2.2. Banda Base

La banda base permite el enlace físico de radiofrecuencia entre dispositivos Bluetooth dentro de una piconet, es decir, dos o más dispositivos Bluetooth que comparten un mismo enlace físico. Como estos terminales utilizan la expansión de espectro por saltos de frecuencia, donde los paquetes se transmiten en franjas de tiempo predefinidas por frecuencias conocidas, este nivel utiliza procedimientos de averiguación y localización para sincronizar la frecuencia de saltos de transmisión y los relojes de los diferentes dispositivos Bluetooth.

Además se encarga de controlar las operaciones sobre los bits y los paquetes, detectar y corregir los errores que se produzcan en el medio, así como de la difusión automática de mensajes a diferentes puntos de la red o del cifrado. También emite confirmaciones y peticiones de repetición de las transmisiones recibidas. Es decir, efectúa las tareas de la capa de enlace del modelo OSI.

3.2.2.1. Enlaces físicos

Corresponden con el nivel más bajo de abstracción dentro de la arquitectura Bluetooth. Se definen cuatro tipos de canales físicos: dos estarán destinados a las comunicaciones entre dispositivos conectados y asociados dentro de una piconet específica; mientras que los otros dos, se destinarán al proceso de descubrimiento y al establecimiento de una conexión. No obstante, los cuatro canales físicos mencionados comparten características comunes como son:

Combinación de una secuencia de saltos en frecuencia pseudo-aleatoria, lo que motiva la reducción de los efectos nocivos de las interferencias.

- Intervalos de tiempos específicos para las transmisiones.
- Código de acceso.
- Codificación de la cabecera de los paquetes.

Por su parte, un dispositivo Bluetooth puede usar solo uno de estos canales físicos en un instante de tiempo dado. Sin embargo, en la norma se contempla la existencia concurrente de múltiples operaciones, es decir, un mismo dispositivo puede encontrarse realizando varias operaciones tales como transmitir datos y estar a la espera de ser descubierto o de que le establezcan una conexión. Para ello se ha usado un sistema de multiplexión por división en el tiempo entre los canales. De esta forma, se consigue transmitir la sensación de que un mismo equipo puede encontrarse conectado simultáneamente en varias piconets mientras está siendo descubierto o esperando el establecimiento de una conexión nueva. En este sentido, algunos dispositivos avanzados pueden ser capaces de conectarse simultáneamente a más de un canal, aunque este hecho no queda recogido en la norma.

A continuación se muestran los diferentes canales físicos definidos en el estándar Bluetooth.

- **Canal físico básico para Piconets.** En el estado “Conexión”, este canal se corresponde con el usado por defecto. Queda definido por el maestro de la piconet que, por definición, se trata del dispositivo que inicia una conexión mediante paging. Además, el maestro será quien se encargue de controlar el tráfico de la piconet mediante un esquema de polling. En este tipo de canales, la secuencia de saltos en frecuencia pseudo-aleatoria hace uso de las 79 frecuencias de RF disponibles y se determinará mediante el reloj del maestro y su dirección Bluetooth. En relación a la división en intervalos de tiempos, estos poseen una duración de 625 microsegundos y son numerados de acuerdo a los 27 bits más significativos del reloj del maestro. El rango de numeración va desde 0 a $2^{27} - 1$ y es un rango periódico con periodo 2^{27} . Por otro lado, el maestro siempre empezará a transmitir en un intervalo de tiempo par, quedando a la espera de recibir datos de los esclavos en los instantes impares. En el caso de usar paquetes cuya transmisión ocupe varias divisiones temporales, se puede conmutar la transmisión por el proceso de recepción. De tal forma que el maestro transmitiría en instantes impares y los esclavos en los pares. A su vez, después de efectuar una transmisión, un paquete de respuesta es esperado durante un tiempo $N \times 625 \mu s$ tras el comienzo de la transmisión. El parámetro N es un número entero e

impar mayor que cero y su valor depende del tipo de paquete que se haya transmitido. Por su parte, en el caso de la recepción, el correlador de acceso buscará un código de acceso correcto en el canal. Si no se obtiene ningún resultado positivo, entonces el receptor esperará hasta el siguiente intervalo de recepción. En caso de producirse una comparación satisfactoria, el receptor quedará pendiente de recibir el resto del paquete salvo que el destinatario no sea ese dispositivo, haya un error irrecuperable en la cabecera o este se produzca en la carga del paquete.

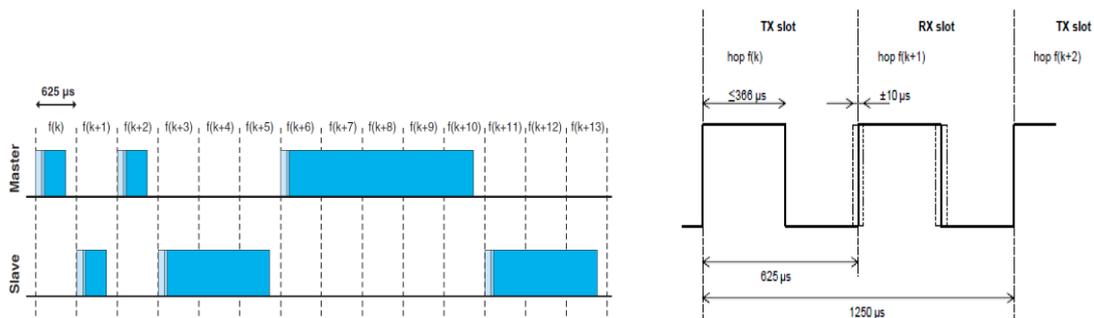


Figura 3.2.1. (a) Transmisión de paquetes multi-intervalos y (b) ciclo de transmisión y recepción de un transceptor maestro en un modo normal de transmisión para paquetes de un solo intervalo.

- Canal físico adaptado para Piconets.** Este tipo de canal se diferencia del anterior en que el número de frecuencias que utiliza es inferior a los 79 definidos por la norma. No obstante, existe un mínimo que canales de RF a usar y se corresponde con 20. Además de este hecho existen una segunda diferencia, es que el mismo mecanismo de canal que hace la frecuencia esclava es el que realiza anteriormente la transmisión maestra.
- Canal físico para Page Scan.** Estos canales se caracterizan por seguir un patrón de salto más lento que los canales físicos para Piconets. Este hecho se debe al uso de una secuencia de salto más pequeña y que es determinada por la dirección Bluetooth del que busca. En cuanto a la temporización del canal físico para Page Scan, esta será determinada por el reloj nativo del terminal que busca los dispositivos. Durante el procedimiento de paging, el maestro transmitirá mensajes relacionados con el dispositivo al que se quiere conectar. En un único intervalo de transmisión, el mensaje se transmitirá en dos frecuencias diferentes como se muestra en la figura 3.2.2. Para el intervalo de recepción, el dispositivo escuchará los mensajes de respuestas en dos frecuencias diferentes.

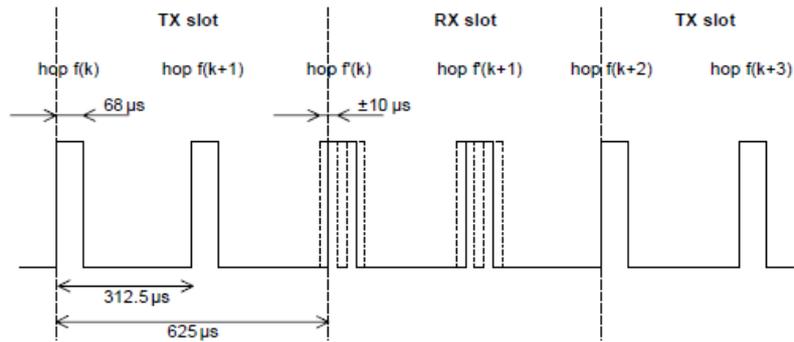


Figura 3.2.2. Ciclo Rx/Tx de un transceptor en modo Page. En ella, $f(k)$ se usa para las frecuencias de la secuencia de salto correspondientes a la transmisión y $f'(k)$, para las de recepción.

- Canal físico para Inquiry Scan.** Estos canales se caracterizan por seguir un patrón de salto más lento que los canales físicos para Piconets. Este hecho se debe al uso de una secuencia de salto más pequeña y que es determinada por la dirección Bluetooth del que busca. En cuanto a la temporización del canal físico para Inquiry Scan, esta será determinada por el reloj nativo del terminal que busca los dispositivos. Durante el proceso de Inquiry o de descubrimiento, el maestro transmitirá mensajes con el código de acceso general o dedicado. Por su parte la temporización para el descubrimiento es equivalente al explicado para el mecanismo de paging.

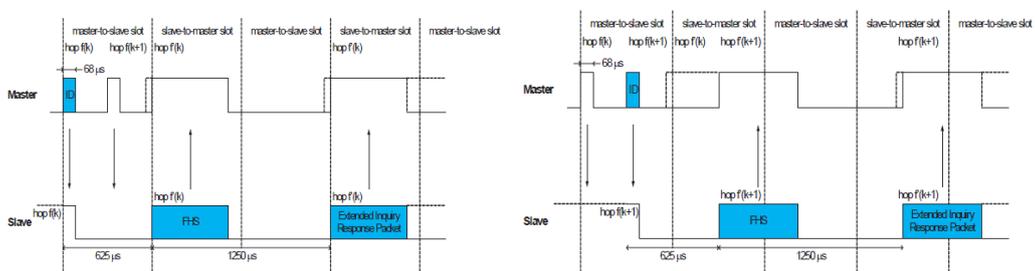


Figura 3.2.3. (a) Temporización de un paquete de respuesta al inquiry con éxito en la primera mitad del intervalo. (b) Temporización de un paquete de respuesta al inquiry con éxito en la segunda mitad del intervalo.

3.2.2.2. Enlaces físicos

Un enlace físico representa una conexión a nivel de banda base entre dispositivos. Éste siempre estará asociado a un solo canal físico.

Por su parte, los enlaces físicos poseen un conjunto de propiedades que son comunes a todos los mecanismos de transporte lógicos. Estas propiedades resultan ser:

- Control de potencia.

- Supervisión del enlace.
- Encriptación.
- Cambio de la tasa de transferencia de datos dada según la calidad del canal.
- Control de paquetes que ocupen varios intervalos temporales.

De las propiedades anteriores cabe destacar la supervisión del enlace debido a que es una tarea crítica. Una conexión puede romperse por motivos tales como que uno de los terminales haya salido fuera de cobertura, existen muchas interferencias en el canal o se haya producido un fallo en la alimentación de algún equipo. Puesto que alguno de estos fallos se produce sin previo aviso, es importante monitorizar el enlace tanto del lado del maestro como del esclavo para evitar posibles colisiones cuando la dirección del transporte lógico o de un miembro en estado park se reasigne a otro esclavo.

Para poder detectar las pérdidas, tanto el maestro como el esclavo usarán un temporizador de supervisión del enlace. Una vez recibido una cabecera de paquete válida con la dirección de un esclavo en el enlace físico, el temporizador se reiniciará. Si en algún instante durante el estado de conexión, el temporizador alcanza su valor límite, $T_{supervision}$, la conexión se considerará desconectada. Este mismo temporizador es el usado para los transportes lógicos ACL, SCO y eSCO.

Finalmente, el valor del temporizador se negocia con el Gestor del enlace, eligiéndose de tal forma que resulte mayor que los periodos asociados a los estados sniff y hold.

3.2.2.3. Transportes lógico

En este apartado se procederá a describir los mecanismos que la especificación Bluetooth posee para ofrecer diferentes servicios que cubran las exigencias de los usuarios. En concreto se definen cinco tipos de transportes lógicos:

Orientado a conexión síncrono (SCO, Synchronous Connection-Oriented). Se caracteriza por ser un enlace punto a punto simétrico entre el maestro y un esclavo específico. Este transporte lógico se basa en la reserva de intervalos de tiempos, lo que permite emular una conexión basada en conmutación de circuitos, ya que dicha reserva es permanente mientras el enlace exista. El maestro puede soportar hasta tres enlaces SCO a un mismo esclavo o a varios. Por su parte, un esclavo puede llegar a mantener hasta tres enlaces con un

mismo maestro o dos enlaces si estos proceden de maestros diferentes, lo que implicaría que el dispositivo esclavo estaría inmerso en varias piconets.

Orientado a conexión síncrono extendido (eSCO, extended Synchronous Connection-Oriented). Este segundo tipo de enlace síncrono se corresponde con un transporte lógico punto a punto entre el maestro y un esclavo específico. Sin embargo, a diferencia de SCO, el enlace puede ser simétrico a asimétrico, lo que implicaría que el número de intervalos temporales reservados no tiene por qué ser igual entre el maestro y el esclavo que entre el esclavo y el maestro. Este transporte lógico se basa en la reserva de intervalos de tiempos, al igual que SCO, lo que permite emular una conexión basada en conmutación de circuitos. Por otro lado, eSCO soporta una ventana de retransmisión inmediatamente después de los intervalos reservados. La unión de estos intervalos y de la ventana de retransmisión es lo que se conoce como ventana eSCO.

No orientado a conexión asíncrono (ACL, Asynchronous Connectionless Link). Este tipo de transporte lógico permite suministrar un mecanismo de transporte basado en conmutación de paquetes entre el maestro y todos los dispositivos esclavos que constituyan la piconet, incluidos aquellos que ya poseen un enlace SCO y/o eSCO activo. Para ello hace uso de los intervalos de tiempo no reservados por los enlaces SCO y eSCO. Por su parte, entre un maestro y un esclavo tan sólo puede existir un enlace ACL.

Difusión para esclavos activos (ASB, Active Slave Broadcast). Este transporte lógico se usa cuando el maestro quiere comunicarse con todos los esclavos activos. No existen asentimientos debido a que el tráfico es unidireccional desde el maestro de la piconet a los esclavos. Sólo puede ser usado por el tráfico de grupo L2CAP. Nunca se utilizará por los canales orientados a conexión de L2CAP, señalización de control L2CAP o por la de LMP.

Difusión para esclavos en estado parked (PSB, Parked Slave Broadcast). Este transporte lógico se usa cuando el maestro quiere comunicarse con los esclavos que han sido puestos en estado parked. Este mecanismo de transporte resulta más complejo que los anteriores por lo que se lleva a cabo en varias fases, cada una de las cuales posee una finalidad diferente. Estas fases son:

- **Información de control:** usada para transportar los enlaces lógicos LMP.
- **Información de usuario:** utilizada para transportar los enlaces lógicos de L2CAP.
- **Fase de acceso:** transporta la señalización de la banda base.

3.2.2.4. Enlaces lógicos

Los enlaces lógicos se definen como el nivel de la arquitectura más bajo usado para ofrecer servicios de transporte de datos a los diferentes usuarios de Bluetooth. En la especificación se definen cinco tipos de enlaces:

- **Control del enlace (LC, Link Control).** Sirve para transportar información de control del enlace como ARQ, control de flujo y la caracterización de la carga. Se transporta en todos los paquetes excepto en el paquete ID que no tiene cabecera.
- **Control ACL (ACL-C, ACL Control).** Se utiliza para transportar la información de control intercambiada entre el gestor de enlaces del maestro y de los esclavos.
- **Usuario asíncrono/isócrono (ACL-U, User Asynchronous/Isochronous).** Se usa para transportar los datos de usuario L2CAP asíncrono e isócrono. Estos paquetes pueden ser transmitidos en uno o más paquetes de la banda base.
- **Usuario síncrono (SCO-S, User Synchronous).** Se emplea para transportar de forma transparente los datos de usuario síncronos. Sobre el viajan el transporte lógico SCO.
- **Usuario extendido síncrono (eSCO-S, User Extended Synchronous).** Se destina para transportar de forma transparente los datos de usuario síncronos. Sobre el viajan el transporte lógico eSCO.

3.2.2.5. Código de acceso

Se corresponde con el primer campo que aparece en todos los paquetes Bluetooth. La estructura genérica de estos se representa en la figura 3.2.4, tanto para modo básico de transferencia como para el modo EDR.

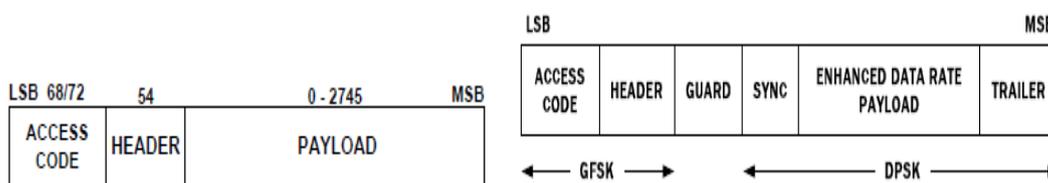


Figura 3.2.4. (a) Estructura de un paquete genérico para el modo básico y (b) Estructura de un paquete genérico para el modo EDR.

La misión del código de acceso es identificar todos los paquetes intercambiados en un canal físico de forma que todos los paquetes que se envíen por el mismo canal físico estén precedidos del mismo código de acceso. Además, se usa también para sincronización y compensación del offset de la tensión continua.

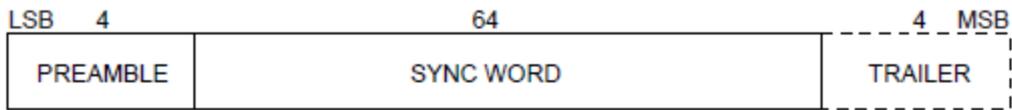


Figura 3.2.5. Formato del código de acceso.

Existen dos tipos de códigos de accesos, uno corto, que ocupa 68 bits y que está compuesto únicamente de un preámbulo y una palabra de sincronización, y otro largo, que añade un tercer campo denominado trailer y cuya longitud se incrementa hasta los 72 bits.

Por otro lado, en la especificación se definen diversos tipos de códigos de accesos. Las diferencias entre ellos radican en las diferentes formas en las que usan la parte más baja de la dirección Bluetooth (representada en la norma por sus siglas inglesas: LAP, Lower Address Part) para construir la palabra de sincronización.

Tipo de código	LAP usado	Longitud [bits]
CAC	Maestro	72
DAC	Dispositivo con el que se ha iniciado una conexión	68/72
GIAC	Reservado	68/72
DIAC	Dedicado	68/72

Tabla 3.2.2. Resumen de los tipos de códigos de acceso diferentes especificados en la norma.

En relación al preámbulo consiste en un patrón de ceros y unos de 4 símbolos usados para facilitar la compensación en continua. La secuencia utilizada es 1010 si el bit menos significativo de la palabra de sincronización comienza por 1 ó 0101, si empieza por cero.



Figura 3.2.6. Preámbulo.

Con respecto a la palabra de sincronización, ésta está compuesta por un código de 64 bits derivado de los 24 bits que componen el LAP. La forma en la que se construye dicha palabra garantiza una gran distancia de Hamming ($d_{min} = 14$) entre las diferentes palabras de sincronización generadas a partir de los distintos LAPS.

Finalmente, el tráiler es un apéndice a la palabra de sincronización cuando la cabecera del paquete sigue al código de acceso. Esta suele ser la situación del código de acceso CAC, aunque también suele darse en el DAC y el IAC cuando estos códigos se usan en los paquetes FHS intercambiados durante una respuesta de tipo page o inquiry. Está compuesto de un patrón de ceros y unos de cuatro símbolos. De manera que con los tres bits más significativos de la palabra de sincronización forman un conjunto de 7 bits de unos y ceros alternos que puede usarse para extender la compensación de DC.

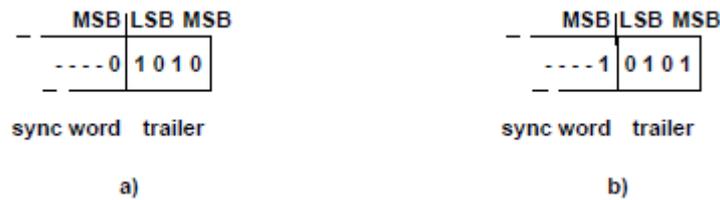


Figura 3.2.7. (a) Trailer en CAC cuando el bit más significativo es cero y (b) trailer en CAC cuando el bit más significativo es uno.

3.2.3. Operación del controlador de enlaces

En esta sección se procederá a describir cómo se establece una piconet y cómo los dispositivos pueden sumarse y retirarse de dicha piconet. También se discutirá el funcionamiento de las scatternets, o redes compuestas con miembros que pertenecen a varias piconets a la vez.

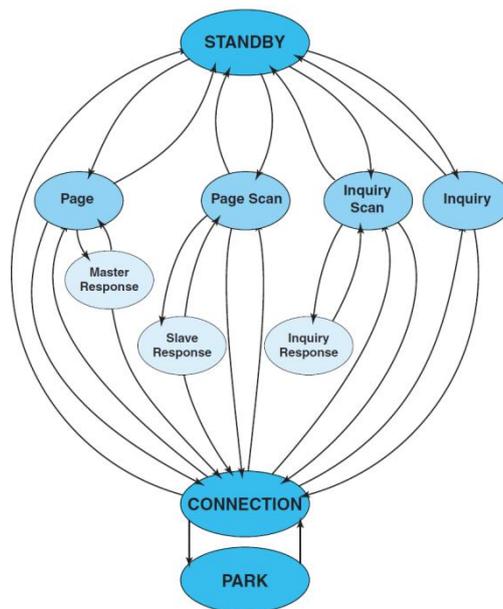


Figura 3.2.8. Diagrama de estados del controlador de estados.

Para moverse de un estado o subestado a otro, se utilizan los comandos del gestor de enlaces o señales internas del controlador, como puede ser la señal de disparo del correlador y las señales de vencimiento de los temporizadores.

En relación al estado Standby, este se caracteriza por ser el estado por defecto en el dispositivo. En él, el terminal puede encontrarse operando en un modo de bajo consumo donde únicamente se encuentra el reloj en funcionamiento. Este estado puede ser abandonado para pasar al subestado Page, Page Scan, Inquiry o Inquiry Scan.

Con respecto al estado de conexión, se corresponde con el estado donde la conexión entre dos dispositivos se ha establecido y el intercambio de paquetes puede comenzar. En ambos dispositivos se utiliza el código de acceso del canal (CAC, impuesto por el maestro) y el reloj nativo del maestro. A su vez, en este estado se puede usar la secuencia de salto de canal básica o adaptada, en cuyo caso se necesitaría el mapa de canales AFH.

El estado de conexión empieza con un paquete POLL enviado por el maestro para verificar el cambio de la temporización de él y los saltos de canal. El esclavo puede responder con cualquier tipo de paquete. Si no respondiera o el maestro no recibiese respuesta por parte del esclavo, ambos dispositivos pasarían al subestado Page o Page Scan.

Por su parte, el primer paquete transmitido en el estado de conexión contiene información de control que permite caracterizar el enlace y dar más detalles de los dispositivos conectados. Estos mensajes serán intercambiados entre los gestores de enlaces de ambos dispositivos.

Para informar de la salida del estado Connection, se usan los comandos detach o reset. En el caso de que el enlace se haya desconectado de manera normal, se usará el comando detach. Mientras que el comando reset queda reservado para un reinicio del controlador de enlaces. Después de que este haya sido completado, la operación que estuviese ejecutándose se perderá.

Por otro lado, en el estado de conexión, un dispositivo no tiene por qué estar siempre presente en el canal y puede declararse no disponible a través de los modos de funcionamiento Sniff o Hold.

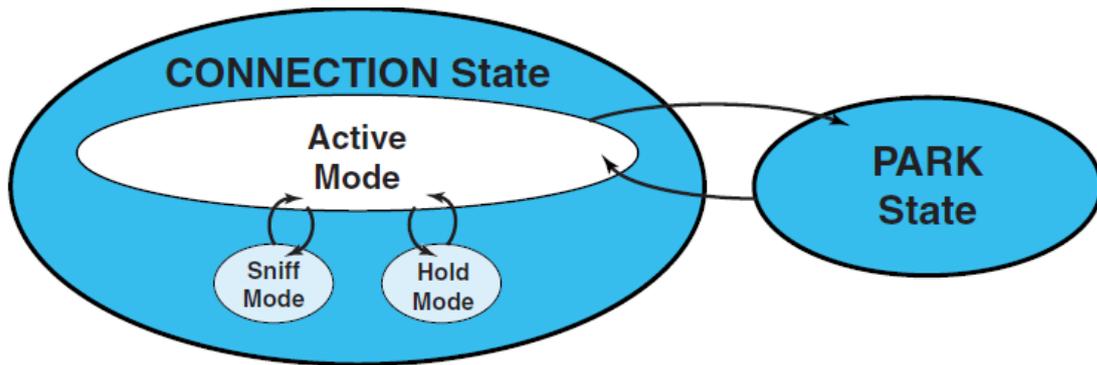


Figura 3.2.9. Representación detallada del estado Connection.

Por tanto, dentro del estado Connection se pueden encontrar tres modos de funcionamiento del dispositivo diferentes, como puede observarse en la figura 3.2.9. Estos modos serán:

- **Modo activo.** En este estado, tanto el maestro como el esclavo participan en el canal. Hasta siete esclavos pueden encontrarse en el modo activo en un mismo instante de tiempo. El maestro será quién planifique los tiempos de transmisión asignados a cada uno según la demanda de tráfico hacia y desde los distintos esclavos. Además, soporta transmisiones regulares para almacenar los esclavos sincronizados. Estos dispositivos se conocen como esclavos activos. Si un esclavo activo no es direccionado, puede retirarse hasta la próxima nueva transmisión del maestro. Por su parte, cuando un dispositivo está participando en múltiples piconets, debe escuchar en el intervalo de tiempo de transmisión del maestro al esclavo correspondiente. Se recomienda que un dispositivo no abandone una piconet en la que está participando más de T_{poll} intervalos de tiempo.
- **Modo Sniff.** Durante este modo, el ciclo de actividad del esclavo en la piconet puede ser reducido. Por ejemplo, se puede pensar en un esclavo que se encuentra en modo activo sobre un enlace ACL. Él escuchará en todos los intervalos de tiempos ACL del tráfico del maestro, a menos que se trate de un enlace perteneciente a una scatternet o esté ausente debido al modo Hold. Si este dispositivo se encontrase en modo sniff, los intervalos de tiempos que el esclavo estaría escuchando se verían reducidos, de forma que el maestro solo transmitiría en unos intervalos específicos. Dichos intervalos estarán separados por un tiempo T_{sniff} .

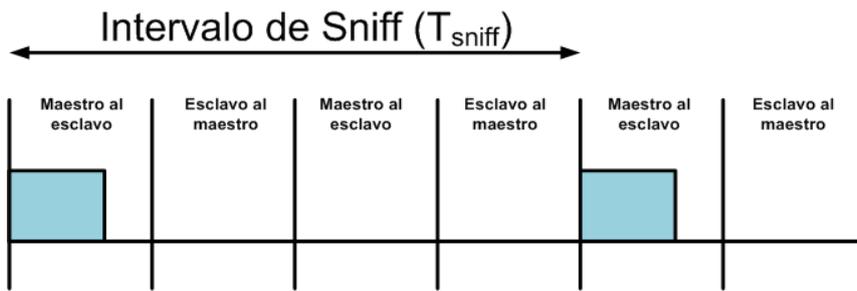


Figura 3.2.10. Esquema temporal del funcionamiento del modo Sniff.

- Modo Hold.** Cuando un dispositivo entra en modo Hold provoca que, temporalmente, no se puedan recibir paquetes ACL. No obstante, cualquier paquete asociado a un enlace síncrono (SCO o eSCO) será soportado. Esto permite al dispositivo en modo hold, poder realizar otras tareas como descubrir nuevos dispositivos o atender a otra piconet. También puede ser utilizado para hacer entrar al dispositivo en un modo de bajo consumo. Durante este modo, el esclavo almacena su dirección de transporte lógica. Por otro lado, antes de poder entrar en modo hold, el maestro y el esclavo tiene que ponerse de acuerdo en la duración del intervalo de tiempo que el esclavo permanecerá en dicho modo. De esta forma, cuando el esclavo se pase al modo hold, se iniciará un temporizador con dicho valor. Cuando éste expire, el esclavo despertará y se sincronizará a la piconet esperando nuevas transmisiones del maestro.

En la figura 3.2.8 se muestra el diagrama de estados del controlador de enlaces y cómo se puede acceder a cada uno de ellos. En él se observan tres estados principales denominados standby, connection y park. Además de estos tres estados, existen siete subestados utilizados para el establecimiento de conexiones y para el descubrimiento de los dispositivos Bluetooth existentes en el rango de cobertura. Estos siete subestados se corresponden con:

- Page.** Se trata de un subestado utilizado por el maestro (fuente) para activar y conectar a un esclavo (sumidero) en el subestado page scan. El maestro intenta coincidir con la actividad de exploración del esclavo, transmitiendo repetidamente los mensajes de paging consistentes en el código de acceso del dispositivo esclavo en diferentes canales. Puesto que el reloj del maestro y del esclavo no están sincronizados, el maestro no conoce exactamente cuando el esclavo despertará ni en que salto de frecuencia. Por tanto, el maestro

transmite un tren de idénticos mensajes de page scan en diferentes frecuencias y escucha entre los intervalos de transmisión hasta que recibe una respuesta del esclavo.

El maestro comunica la dirección Bluetooth del esclavo al controlador. Ésta se usará por el maestro para determinar la secuencia de saltos del subestado page. Para la fase de la secuencia, el maestro usará una estimación del reloj del esclavo. Aunque el maestro y el esclavo usen la misma secuencia de saltos, la fase puede ser diferente, de forma que el esclavo y él no se sincronicen. Por este motivo, el maestro transmite varios mensajes page durante un intervalo corto de tiempo en un conjunto de frecuencias activas. Durante cada intervalo de transmisión, el maestro transmitirá secuencialmente en dos frecuencias diferentes. En el siguiente intervalo de recepción, el receptor escuchará secuencialmente en dos frecuencias diferentes.

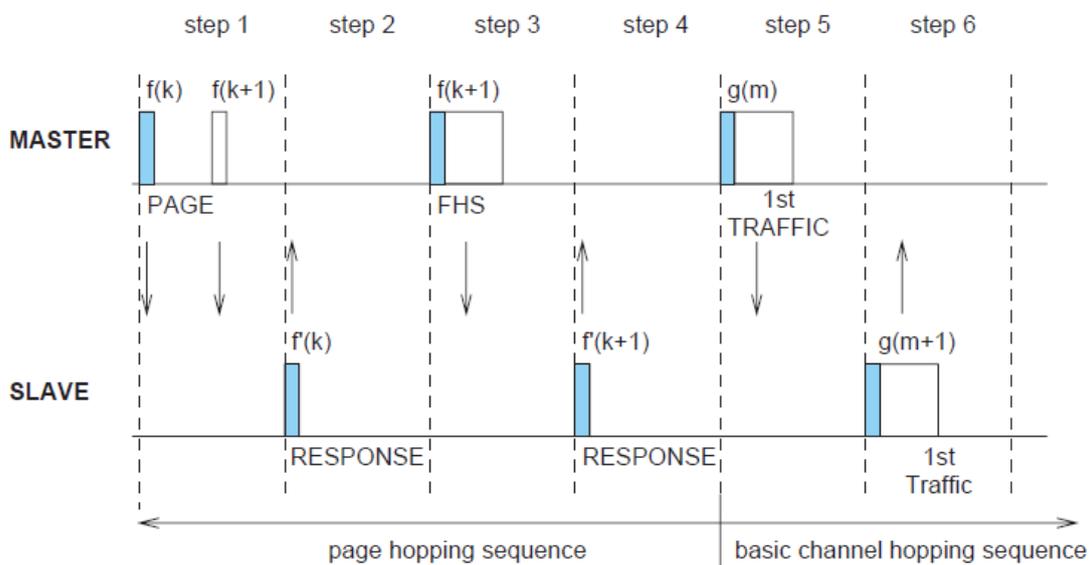


Figura 3.2.11. Intercambio de mensajes durante la fase inicial de la conexión cuando un esclavo responde un primer mensaje page.

El subestado page se puede acceder desde el estado Standby o Connection.

- **Page Scan.** Se corresponde con un estado donde un dispositivo puede ser configurado para usar un procedimiento de exploración estándar o entrelazado con el fin de establecer una conexión. Durante una exploración

normal, el dispositivo escucha durante una ventana de tiempo $T_{w_page_scan}$ (11,25 ms por defecto), mientras que la exploración entrelazada se mejora con dos exploraciones, una tras otra, de $T_{w_page_scan}$. Por este motivo, si el intervalo de exploración no es al menos dos veces la ventana de exploración, el modo entrelazado no se podrá usar. Durante esta ventana, el dispositivo escuchará en una única frecuencia, mientras su correlador espera encontrar su código de acceso de dispositivo (DAC). La ventana de exploración deberá ser lo suficientemente larga como para que dé tiempo a completar la exploración de 16 frecuencias. Cuando el dispositivo entra en este estado, seleccionará la frecuencia de exploración de acuerdo a la secuencia de saltos determinada por la dirección Bluetooth del dispositivo. La fase de la secuencia se determinará por los bits 12, 13, 14, 15 y 16 del reloj nativo del dispositivo. Cada 1.28 segundos se seleccionara una frecuencia diferente. Este estado puede ser accesible desde los estados Standby, Connection.

- **Master Response.** Se corresponde con el subestado en el que entra el dispositivo maestro cuando recibe un mensaje de respuesta page por parte del esclavo. Si se revisa la figura 3.2.11, se podrá comprobar que se corresponde con el paso 2. En esta situación, se congelará en el maestro el valor actual del reloj que se usa como entrada en el esquema de selección de salto para el subestado page. Este valor, se transmitirá en un paquete FHS (véase la figura 3.2.13 para más detalles del contenido del paquete) con destino el terminal esclavo. En él, se halla toda la información necesaria para construir el código de acceso al canal (CAC) sin requerir operaciones matemáticas para derivar la dirección de acceso del dispositivo Bluetooth maestro. El paquete FHS se transmitirá en el comienzo del siguiente intervalo de tiempo entre el maestro y el esclavo tras la respuesta del esclavo.

Después de que se haya enviado, se esperará durante un segundo un mensaje de respuesta por parte del esclavo como asentimiento de la correcta recepción del paquete FHS. Esta respuesta contendrá el DAC del dispositivo esclavo. Si no se recibe respuesta, el maestro retransmitirá el paquete FHS con un valor actualizado del reloj y usando aún los parámetros del esclavo cada vez hasta que se reciba un segundo mensaje de respuesta o el temporizador asociado al tiempo de espera de una respuesta cumpla. En este último caso, el

maestro volverá al subestado page y enviará un error al gestor de recursos de la bandabase.

Por su parte, si la respuesta del esclavo se recibe, el maestro usará sus parámetros, es decir, pasará a utilizar su CAC y su reloj. Finalmente, el maestro entrará en el estado de Connection.

- **Slave Response.** Este subestado se corresponde con el estado del controlador de enlaces para responder un mensaje de tipo page. Como se puede observar en la figura 3.2.11, después de recibir el mensaje page en el paso 1, el esclavo transmitirá una respuesta que contiene su código de acceso de dispositivo, es decir, deberá responder con su DAC. Dicho mensaje de respuesta, se generará $625 \mu s$ después de recibir el mensaje page del paso 1. Acto seguido, el esclavo activará su receptor transcurridos $312.5 \mu s$ desde el comienzo del mensaje de respuesta, a la espera de recibir un paquete FHS.

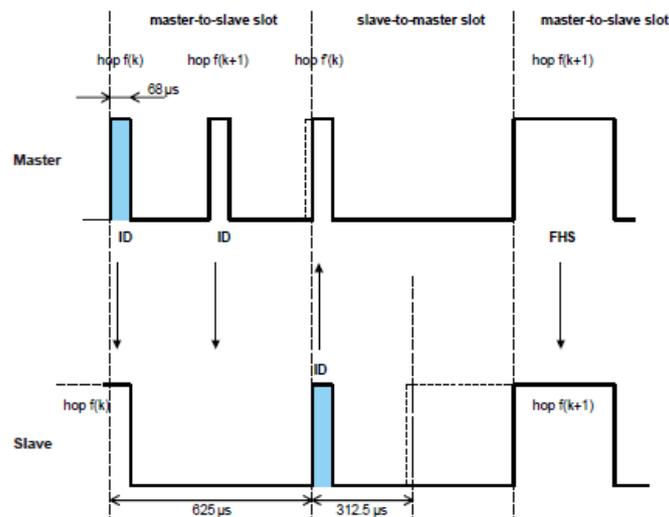


Figura 3.2.12. Temporización de los paquetes de respuestas en el subestado page.

Si un paquete FHS se recibe en este subestado dentro de los límites temporales establecidos, el esclavo responderá con mensaje para asentar la recepción de dicho paquete. En ese instante, el esclavo cambiará al CAC del maestro y modificará el reloj en base al recibido en el paquete FHS. Finalmente, el esclavo entrará en el estado Connection, usando el reloj y la dirección Bluetooth del maestro para determinar la secuencia de salto en frecuencia y el CAC.

Por el contrario, si la configuración de la conexión falla antes de que el estado Connection sea alcanzado, el esclavo estará escuchando en el canal siempre y cuando no se haya recibido un paquete FHS o el temporizador asociado a la recepción de un mensaje de respuesta venza. No obstante, cada 1.25 ms , deberá seleccionar la siguiente secuencia de salto en frecuencia con dirección maestro-esclavo. Si no se recibe nada después de que se cumpla nuevamente dicho temporizador, el esclavo deberá devolver al subestado page scan durante un periodo de búsqueda.

- **Inquiry.** Este subestado se usa para descubrir a nuevos dispositivos. Es muy similar al subestado Page. En concreto, las temporizaciones asociadas a la transmisión y a la recepción serán las mismas. Con respecto a las frecuencias de transmisión y de recepción, éstas seguirán la secuencia de salto de inquiry y de inquiry response, que se determinarán por el GIAC y el código nativo de reloj del dispositivo que realiza el proceso de descubrimiento. Por su parte, entre cada transmisión, se buscarán mensajes de respuestas (paquete FHS). Cuando una respuesta se reciba, el paquete entero se procesará. Si el bit EIR del paquete FHS se encuentra fijado a uno, quiere decir, que se tratará de una respuesta extendida y se deberá esperar $1250\ \mu\text{s}$ tras la recepción de la respuesta para recibir la respuesta extendida. Todos estos paquetes no se asentarán.

Bits de paridad	LAP	EIR	No definido	SR	Reservados	UAP	NAP	Clase del dispositivo	LT_ADDR	CLK ₂₇₋₂	Modo Page Scan
-----------------	-----	-----	-------------	----	------------	-----	-----	-----------------------	---------	---------------------	----------------

Figura 3.2.13. Formato del paquete FHS.

Por otro lado, de este subestado tan solo se puede salir de tres formas diferentes:

- El gestor de recursos de la base de datos genera un comando de parada tras alcanzar un número de respuestas especificado. En caso de no especificar dicho valor, el gestor de recursos no podrá solicitar la salida del subestado.
- El temporizador asociado al tiempo de descubrimiento vence.
- El host que alberga al dispositivo Bluetooth decide cancelar el descubrimiento mediante el envío de un comando.

Al subestado de inquiry se puede acceder desde los estados standby o connection. No obstante, antes de poder acceder al inquiry desde el estado Connection, el dispositivo debe liberar tanta capacidad del enlace como le sea posible para poder llevar a cabo la búsqueda de nuevos terminales. Para garantizar esta premisa, en la especificación se aconseja utilizar los modos sniff, hold o park. Sin embargo, los intervalos de tiempos asignados a las conexiones síncronas no se verán perturbados por el proceso de descubrimiento. De hecho, se interrumpirá para poder transmitir en los intervalos de tiempo reservados para los enlaces SCO y eSCO, puesto que son más prioritarios que la acción de descubrir nuevos dispositivos.

- **Inquiry Scan.** En este subestado se lleva a cabo la tarea de buscar el código de acceso IAC durante un período lo suficientemente largo como para completar dicha búsqueda en las 16 frecuencias asignadas. Resulta similar al subestado page scan, salvo que en vez de buscar dispositivos por el DAC, se hace mediante el IAC. Existen dos tipos de búsquedas, la normal y la entrelazada. En el caso de una búsqueda normal, la longitud del período de búsqueda se denota por $T_{w_inquiry_scan}$ y las frecuencias donde realizarla se determinan por Xir_{4-0} . Para el modo entrelazado de búsqueda, lo que se hace es mejorar el proceso de búsqueda mediante dos exploraciones en diferentes frecuencias, una se efectúa en el salto de frecuencia definido por el modo normal y el otro se realiza en $[Xir_{4-0} + 16] \bmod 32$. Para que se pueda ejecutar de forma correcta, es necesario que el intervalo de búsqueda sea al menos dos veces $T_{w_inquiry_scan}$. Además, la fase es determinada por el reloj nativo del dispositivo que se encuentra en este subestado, cambiando cada 1.28 segundos.

Este subestado puede ser accedido desde los estados standby y connection. Al igual que sucede en el estado inquiry, el dispositivo deberá reservar toda la capacidad posible.

- **Inquiry Response.** Se trata del subestado de respuesta a los mensajes de inquiry. No puede enmarcarse dentro del subestado Slave Response, debido a que este último se aplica sólo como respuesta a los mensajes page. Cuando el mensaje inquiry se recibe en el subestado inquiry scan, el receptor devolverá

un paquete FHS como respuesta conteniendo la dirección Bluetooth del dispositivo y otros parámetros. En el caso de que el receptor estuviera esperando una respuesta extendida, se enviaría la respuesta extendida transcurrido el tiempo necesario tras el paquete FHS de respuesta. El mecanismo implementado en el esclavo será el siguiente:

- En el primer mensaje inquiry recibido en el subestado inquiry scan, el esclavo entrará en el subestado inquiry response.
- Si el esclavo está configurado para devolver un mensaje de respuesta extendida, en el paquete FHS de respuesta, el bit EIR se encontrará fijado a uno. Pasados $1250 \mu s$, responderá con el mensaje de respuesta extendida.
- En caso contrario, el dispositivo esclavo responderá únicamente con el paquete FHS.
- En el caso de que existan muchos dispositivos Bluetooth, correctamente configurados, en las proximidades del terminal que está efectuando el proceso de descubrimiento, puede surgir un problema si todos los dispositivos intentan responder a la vez el mensaje de inquiry. Sin embargo, debido a que cada dispositivo tiene un reloj corriendo arbitrariamente, es poco probable que todos ellos usen la misma fase en la secuencia de salto del proceso de descubrimiento. Para evitar colisiones repetitivas, se ha implementado un sistema de espera aleatorio. Si el dispositivo recibe un mensaje inquiry y responde con un paquete FHS, generará un número aleatorio entre 0 y un número máximo. Este último puede ser de 1023 para intervalos de búsquedas mayores que 1.28 segundos o tan pequeño como 127 si el intervalo es inferior a 1.28 segundos.

Por su parte, tras salir de este subestado, el dispositivo podrá volver al estado de connection o standby, aunque antes de realizar este paso se permite la transición hacia el subestado page scan.

3.2.4. LMP

Cuando dos dispositivos Bluetooth son descubiertos en el rango de cobertura de ambos y deciden establecer una conexión entre ellos, los gestores de enlaces (en inglés, Link Manager, LM) de ambos dispositivos interactúan entre sí intercambiando una serie de

mensajes para gestionar y controlar el la comunicación entre ellos. Al conjunto de mensajes que intercambian bajo una serie de reglas se conoce como Protocolo de Gestión de Enlaces (en inglés, Link Manager Protocol, LMP) y se usa para controlar y negociar todos los aspectos de las conexiones Bluetooth entre dos dispositivos. Esto incluye la configuración y control de enlaces y transportes lógicos y el control de los enlaces físicos. En este punto cabe destacar que todos los mensajes LMP se aplicarán exclusivamente al enlace físico y a los enlaces y transportes lógicos asociados a la comunicación establecida entre el dispositivo emisor y el receptor, y viceversa.

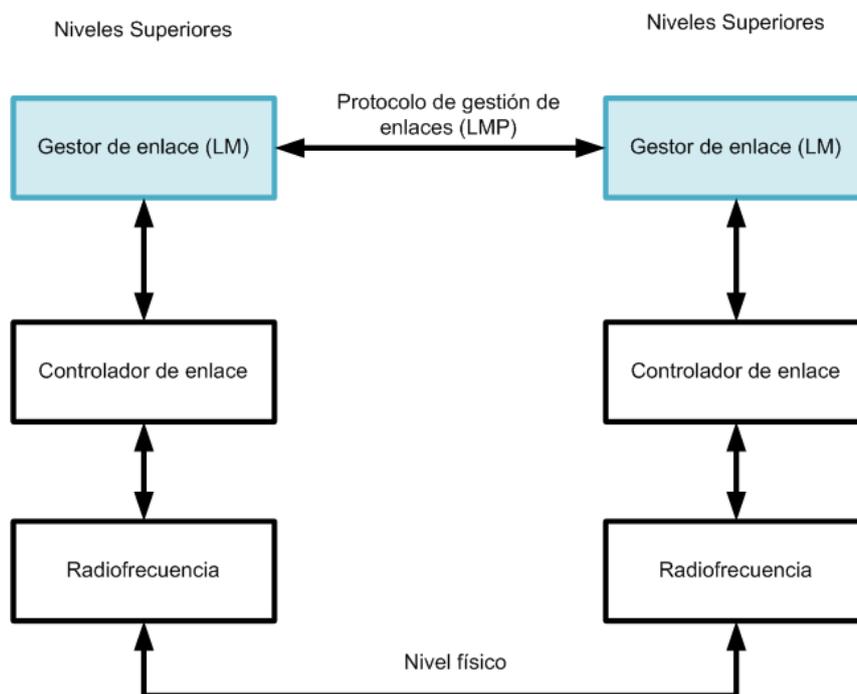


Figura 3.2.14. Operación del protocolo de gestión de enlaces.

Algunos de los servicios soportados por LMP son:

- Transmisión y recepción de datos.
- Petición de nombre.
- Petición de las direcciones de enlace.
- Establecimiento de la conexión.
- Autenticación
- Negociación del modo del enlace y establecimiento. Esta característica puede variar en el transcurso de una conexión.

Este protocolo está constituido por un conjunto de mensajes, denominados PDU, que serán intercambiados sobre enlaces lógicos de tipo ACL-C en los transportes lógicos ACL. Dichos mensajes poseen una prioridad más alta que los datos de usuario, para que un mensaje que necesite enviar el gestor de enlaces no se vea retrasado por el tráfico de los protocolos superiores, como L2CAP. Sin embargo, sí que es posible que las PDU's se vean retrasadas por las retransmisiones múltiples de paquetes de bandabase individuales. En cualquier caso, el gestor de enlaces filtra e interpreta estos mensajes en el lado receptor por su entidad par y no se propaga a los niveles superiores. Las capacidades de detección y corrección del transporte lógico ACL son, en general, suficientes para los requisitos de LMP. Por tanto, las PDU's no contienen ninguna información adicional para informar de la detección de errores más allá de las que puedan realizarse a través de los controles realizados al contenido de los mensajes de LMP.

Por su parte, existen 56 PDU's definidas en la especificación Bluetooth, cada una de las cuales, se utiliza para llevar a cabo una función diferente. A cada PDU se le asigna un código de operación de 7 ó 15 bits que permite identificar de forma unívoca los diferentes mensajes. Los primeros 7 bits del código de operaciones y un identificador de transacción son localizados en el primer byte de la carga. Si el campo asociado al código de operación tiene un valor comprendido entre 124 y 127, entonces se le añade un byte adicional en la carga para generar un código de operación de 15 bits. El resto de parámetros que pueda contener la PDU se ubicarán en los bytes siguientes.

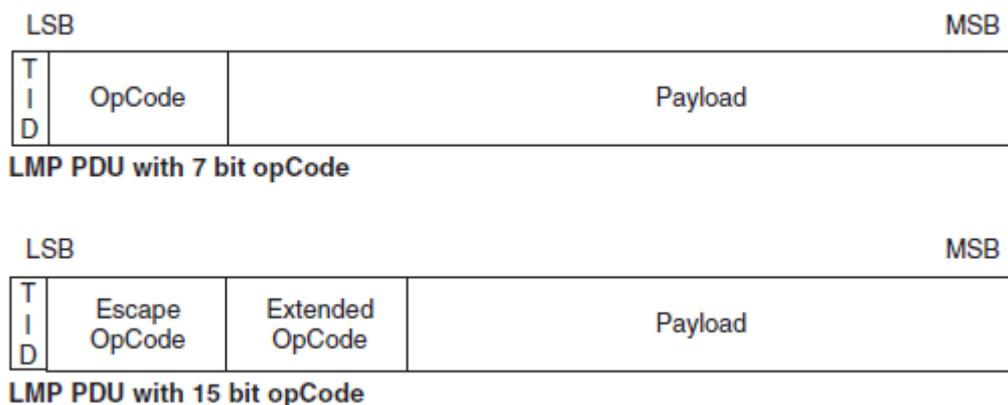


Figura 3.2.15. Estructura de las PDU's intercambiadas por los gestores de enlace.

Cada PDU puede ser de carácter obligatorio u opcional. Desde este punto de vista, el gestor de enlaces no requiere transmitir una PDU opcional, pero deber ser capaz de reconocer todas las PDU, obligatorias u opcionales, y, si se requiere una respuesta, enviar una

contestación válida, incluso cuando se trate de una característica que no esté soportada. No obstante, es posible solicitar una lista de cuáles de las PDU's opcionales están soportadas.

Finalmente, LMP opera en términos de transacciones. Una transacción hace referencia a un conjunto de mensajes intercambiados entre dos dispositivos con una finalidad particular. Todas las PDU's que forman parte de la misma transacción deberán tener el mismo identificador que se almacena como parte del primer byte del código de operaciones. Éste se encuentra en el bit menos significativo. Valdrá "0" si la PDU forma parte de una transacción iniciada por el maestro y "1" en caso contrario, es decir, si la transacción fue iniciada por el esclavo.

3.2.4.1. Modos de operación

Existen tres modos de operación diferentes:

- **Modo de retención (Hold mode):** el transporte lógico ACL de una conexión entre dos dispositivos Bluetooth se puede poner en modo de retención durante un tiempo especificado. Durante este tiempo, el maestro no puede transmitir paquetes. Normalmente, se activa este modo cuando no hay necesidad de enviar datos durante un período relativamente extenso. Durante dicho período, se puede apagar el transceptor para ahorrar energía. No obstante, este modo también se puede utilizar si el dispositivo necesita descubrir nuevos terminales o ser descubierto por otros dispositivos. Finalmente, tanto el maestro como el esclavo pueden solicitar entrar en modo retención.
- **Modo de escucha selectiva (Sniff mode):** se corresponde con otro modo de funcionamiento que permite ahorrar energía en los dispositivos Bluetooth. Para entrar en el modo de escucha selectiva, el maestro y el esclavo negocian un intervalo y un desplazamiento de escucha selectiva, que especifica la temporización de las franjas de escucha selectiva. Después de eso, las franjas de escucha selectiva continúan de forma periódica con el intervalo especificado. Cuando el enlace se encuentra en este modo, el maestro sólo puede iniciar una transmisión en dicha franja. Por su parte, existen dos parámetros que controlan la actividad de escucha en el esclavo:
 - **Duración de la escucha selectiva:** determina durante cuántas franjas debe escuchar el esclavo, comenzando por la de escucha selectiva,

incluso si no recibe un paquete con su propia dirección de miembro activo.

- **Fin de escucha selectiva:** determina cuántas franjas adicionales debe escuchar el esclavo si continúa recibiendo sólo paquetes con su propia dirección de miembro activo.

Finalmente, el maestro puede forzar al esclavo a entrar en modo de escucha selectiva, pero tanto el maestro como el esclavo pueden solicitar por propia voluntad entrar en este modo. Al recibir la solicitud, se puede devolver la misma con los parámetros modificados, o se puede finalizar la negociación.

- **Modo de aparcamiento (Park mode):** si no es necesario que un esclavo participe en el canal, pero aun así debe mantenerse sincronizado con los saltos en frecuencias, se puede colocar al esclavo en modo de aparcamiento. En él, el dispositivo abandona su dirección de miembro activo. Por otro lado, cuando se coloca un esclavo en modo aparcado, se le asigna una dirección de miembro aparcado exclusiva, que puede ser utilizada por el maestro para desaparcar dicho esclavo. Incluso sin su dirección de miembro activo, el dispositivo puede todavía sincronizarse con el canal despertándose en respuesta a mensajes emitidos a intervalos predeterminados. El maestro también puede cambiar los parámetros del modo de aparcamiento, transferir información de difusión o dejar que el esclavo aparcado solicite acceso al canal.

El maestro puede forzar la entrada en modo aparcamiento. En este procedimiento, el maestro finaliza la transmisión del mensaje actual y luego envía la orden para pasar a modo de aparcamiento. Cuando el esclavo la recibe, finaliza la transmisión que estuviera realizando y responde con un mensaje aceptando la orden. No obstante, el maestro también puede solicitar la entrada en dicho modo en vez de forzarla. Para ello, el maestro finaliza la transmisión y envía una petición de entrada en modo aparcado. Si el esclavo acepta la solicitud para entrar en modo aparcamiento, finaliza la transmisión actual y luego responde con un mensaje de aceptación. Si el esclavo rechaza dicha petición, respondería con una negación. Finalmente, el esclavo puede solicitar ser colocado en modo aparcado. En ese caso, el esclavo finaliza la transmisión del mensaje actual y luego envía al maestro una solicitud de

entrada en modo aparcado. Si el maestro acepta la petición de modo aparcado, finaliza la transmisión del mensaje actual y luego envía la orden de entrada en modo aparcado. Si el maestro rechaza dicho modo, enviaría un mensaje rechazando dicha petición.

3.2.5. HCI

Las siglas inglesas HCI se corresponden con Host Controller Interface y es la parte de la especificación Bluetooth que se encarga de suministrar una interfaz de comandos al controlador de la bandabase y gestor de enlaces, y de acceder al estado del hardware y de los registros de control. En esencia, esta interfaz da un método homogéneo de acceso a las capacidades de la bandabase de Bluetooth. Se divide en tres secciones:

HCI Firmware. Se ubica en el controlador del transceptor Bluetooth. Esta sección implementa los comandos HCI para el hardware Bluetooth mediante acceso a las órdenes de la bandabase, comandos del gestor de enlace y a los registros de control, de estado y de eventos.

La capa de transporte. Se corresponde con la sección del HCI encargado de interconectar al HCI driver con el HCI firmware. Un ejemplo de la capa de transporte podría ser el conjunto de capas que pueden existir entre el controlador HCI en un PC (véase, por ejemplo, la pila BlueZ) y el firmware existente en un transceptor Bluetooth. Todas esas capas intermedias, desde el sistema operativo hasta el mecanismo de comunicación utilizado, USB, UART o RS-232, deben suministrar la capacidad de transferir datos sin un conocimiento exhaustivo de los datos que están siendo transferidos.

HCI driver. Está localizada en el transceptor Bluetooth o puede estar integrada en el equipo que alberga el transceptor. Esta sección hace referencia a la entidad software. El equipo recibirá notificaciones asíncronas de eventos HCI, los cuales se usan para notificar cuando ocurre algún suceso susceptible de ser notificado. Cuando el host descubre que un evento ha tenido lugar, entonces analizará el paquete recibido para determinar el tipo de evento acaecido.

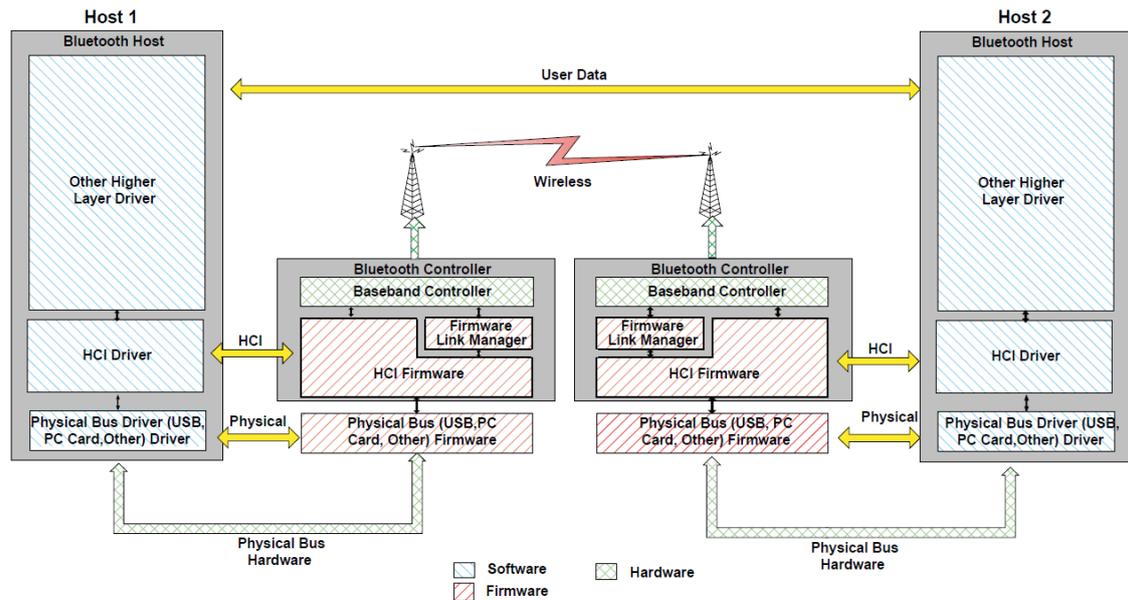


Figura 3.2.16. Información general de extremo a extremo de las capas de software inferiores utilizadas en la transferencia de datos.

3.2.5.1. Comandos HCI

HCI otorga un método homogéneo de acceso, basado en órdenes o comandos, a las capacidades de Bluetooth. Para poder efectuar tal tarea, estos se encuentran ordenados en grupos según la función que realicen. Los diferentes comandos que se pueden encontrar en la norma son:

Grupo	Descripción	Ejemplo
Eventos genéricos	Los eventos genéricos pueden ocurrir debido a múltiples comandos o eventos que pueden suceder en cualquier instante	Command Complete Event
Configuración del dispositivo	Se utilizan para ubicar al Controlador en un estado conocido	Reset Command
Control del controlador de flujo	Se usan para controlar los flujos de datos desde el Host al controlador	Read Buffer Size Command
Información del controlador	Permiten que al Host descubrir información local sobre el dispositivo	Read Local Version Information Command
Configuración del controlador	Dejan configurar los parámetros globales de configuración	Read Local Name Command
Descubrimiento de dispositivos	Son comandos o eventos que consienten a un dispositivo descubrir otros dispositivos que se encuentran en su rango de	Inquiry Command

Configuración de conexiones	cobertura	
	Permiten a un dispositivo realizar una conexión a otro	Create Connection Command
Información remota	Acceden a la información de configuración de un dispositivo remoto que es descubrible	Remote Name Request Command
Conexiones síncronas	Se usan para el establecimiento de conexiones síncronas	Setup Synchronous Connection Command
Estado de la conexión	Obtienen la configuración de un enlace, especialmente utilizados para los enlaces de bajo consumo	Hold Mode Command
Estructura de la Piconet	Permiten descubrir y reconfigurar una piconet	Role Discovery Command
Calidad de servicio	Especifican los parámetros para fijar una determinada calidad en el servicio	Flow Specification Command
Enlaces físicos	Configuran un enlace físico	Read Link Supervision Timeout Command
Control de flujo en el Host	Se utilizan para controlar el flujo de datos hacia el Host	Host Buffer Size Command
Información del enlace	Obtienen información sobre un enlace particular	Read LMP Handle Command
Autenticación y encriptación	Permiten la autenticación de un dispositivo remoto y la encriptación de un enlace	Authentication Requested Command
Pruebas	Se utilizan para poner a un dispositivo en modo de prueba y verificar el comportamiento del mismo	Read Loopback Mode Command

Tabla 3.2.3. Comandos HCI: agrupación y descripción.

3.2.6. L2CAP

Dentro de la especificación Bluetooth, el protocolo L2CAP (Logical Link Control Adaptation Protocol, Protocolo de Adaptación y Control de Enlaces Lógicos) se encarga de la multiplexación de los protocolos de niveles superiores y de las tareas de segmentación y recomposición de paquetes (ver figura 3.2.18). También se encarga de transportar información de calidad de servicio entre un dispositivo y otro. Al igual que LMP, L2CAP se halla en un nivel superior a la bandabase y reside en el nivel de enlace de datos del modelo de referencia OSI.

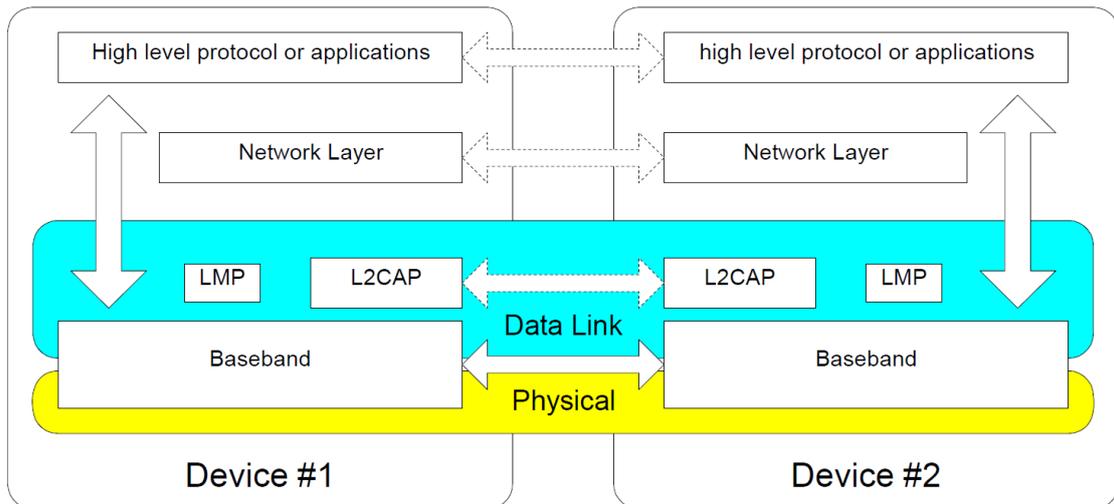


Figura 3.2.17. Ubicación de L2CAP dentro de la torre de protocolos de Bluetooth.

L2CAP permite que las aplicaciones y protocolos de nivel superior transmitan y reciban paquetes de datos de una longitud máxima de 64 KB de longitud. Además, también contempla control de flujo por canal y retransmisiones a través de los modos de control de flujo y retransmisión, respectivamente.

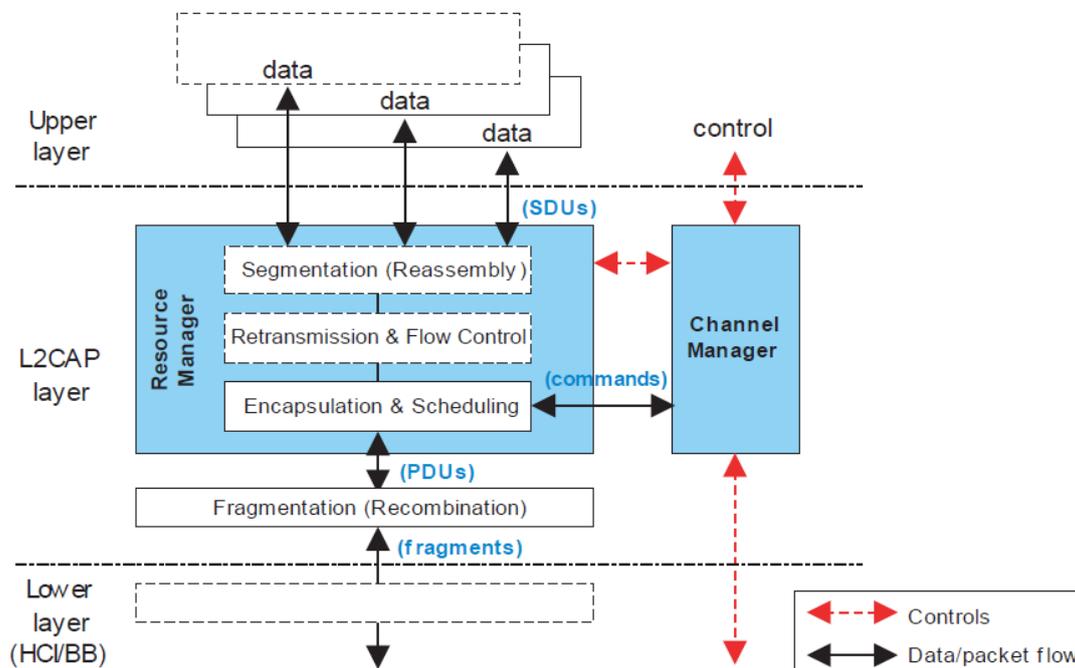


Figura 3.2.18. Diagrama de bloques del protocolo L2CAP.

En otro orden, mientras que en la especificación de la bandabase se definieron dos tipos de enlaces (enlaces síncronos orientados a conexión, SCO, y enlaces asíncronos no orientados a conexión, ACL), el protocolo L2CAP está definido únicamente para enlaces de tipo

ACL y no puede existir nada más que un enlace de este tipo. Esto se debe a que L2CAP depende de las comprobaciones de integridad en el nivel de bandabase para proteger la información transmitida, siendo los enlaces ACL los únicos capaces de satisfacer dichas exigencias a través de un esquema ARQN/SEQN de un bit.

Entre las características de L2CAP están la sencillez y una baja sobrecarga del enlace, lo que le hace apropiado para su implementación en dispositivos con recursos de cálculo y memoria limitados como teléfonos móviles, sistemas empujados o dispositivos PDA. Estas características le permiten alcanzar una elevada eficiencia de ancho de banda sin consumir demasiada energía, de acuerdo con los objetivos de eficiencia energética de la comunicación establecidos en la interfaz radio Bluetooth. Además de su eficiencia, realiza las siguientes tareas:

- **Multiplexación de protocolos y/o canales.** El hecho por el que la multiplexación de los protocolos superiores y de los canales se efectúa por L2CAP se debe a que la bandabase no posee ningún tipo de campo identificativo que permita realizar dicha tarea.
- **Segmentación y reensamblado.** Si L2CAP tiene el control sobre la longitud de las tramas transmitidas, se favorece el funcionamiento de muchas aplicaciones multiplexadas sobre L2CAP. Esto se debe a:
 - La capa de segmentación dejará la separación necesaria entre las unidades de datos de las aplicaciones para satisfacer los requisitos de latencia.
 - La gestión de la memoria y de los buffers se resulta más sencilla cuando L2CAP controla el tamaño de los paquetes.
 - La corrección de errores mediante retransmisiones se puede efectuar de manera más eficiente.
 - La cantidad de datos que se destruye cuando una PDU del protocolo L2CAP se corrompe o se pierde puede hacerse más pequeña que la unidad de datos de la aplicación.
 - La aplicación está desacoplada de la segmentación requerida para encapsular los paquetes de la aplicación en los de las capas inferiores de la especificación Bluetooth.
- **Control de flujo por canal L2CAP.** Este se implementa debido a que el control de flujo de tipo stop-and-go que se usa en la bandabase puede no ser

suficiente para la mayoría de las aplicaciones. Por este motivo, L2CAP también provee un servicio de control de flujo para aplicaciones o perfiles que puedan necesitarlo, sin necesidad que lo implemente estos. El uso de dicho control de flujo es un aspecto opcional del protocolo.

- **Control de errores y retransmisiones.** Algunas aplicaciones requieren una tasa de error residual mucho más pequeña que la suministrada por la base de datos. L2CAP incluye comprobaciones de errores adicionales y retransmisiones de tramas L2CAP.
- **Fragmentación y recombinación.** Las capas inferiores tienen limitada las capacidades de transmisión por lo que podrían requerir el uso de fragmentos de tamaños diferentes a los creados por la subcapa de segmentación de L2CAP. Por tanto, las capas por debajo de L2CAP pueden fragmentar y recombinar PDU's de L2CAP para crear fragmentos que se ajusten a las capacidades de la capa. Durante una transmisión, muchos niveles diferentes de fragmentación y recombinación pueden ocurrir en ambos dispositivos.
- **Calidad de servicio.** Durante el proceso de establecimiento de una conexión L2CAP, se permite el intercambio de información atendiendo a la calidad de servicio esperada entre los dos dispositivos Bluetooth. Cada implementación L2CAP monitoriza los recursos usados por el protocolo y se asegura que la calidad de servicio se satisfice.

3.2.6.1. Modo de operación de L2CAP

L2CAP está basada en torno al concepto de canales. A cada una de las terminaciones de un canal L2CAP se le denomina identificador de canal (Channel Identifier, CID). De esta forma es como se conoce al nombre que representa a una terminación de un canal lógico en un dispositivo. Su alcance es local, es decir, únicamente afecta al dispositivo en cuestión. El conjunto de valores que puede tomar el identificador de canal se representa en la tabla 3.4.

CID	Descripción
0x0000	Identificador nulo. Se corresponde con un identificador ilegal y nunca podrá usarse como una terminación destinataria
0x0001	Canal de señalización
0x0002	Recepción de canales no orientados a conexión

0x0003-0x003F	Reservados para funciones específicas de L2CAP
0x0040-0xFFFF	Asignados dinámicamente

Tabla 3.2.4. Descripción de los diferentes CID que se pueden utilizar.

En relación a la asignación de CID, esta es relativa a un dispositivo en concreto y la asignación de los mismos puede ser totalmente diferente en otro terminal, salvo que se usen los CID's reservados que se muestran en la tabla 3.2.4.

La figura 3.2.19 muestra el uso de varios identificadores CID entre entidades L2CAP situadas al mismo nivel en dispositivos diferentes. Los canales de datos orientados a conexión representan una comunicación entre dos dispositivos, donde un CID identifica a cada extremo del canal. Los canales no orientados a conexión limitan el flujo de datos a una única dirección. Estos canales se utilizan para soportar un "grupo" de canales, donde el CID del origen representa a uno o más dispositivos remotos. En una entidad L2CAP, es obligatorio el soporte de un canal de señalización que permita crear y establecer canales orientados a conexión y negociar cambios en las características de los canales orientados y no orientados a conexión. Además de todos estos CID, se reserva uno más para todo el tráfico entrante de canales de datos no orientados a conexión. En la figura, se utiliza un CID para representar un grupo formado por los dispositivos 3 y 4. El tráfico que se envía desde este CID se dirige al canal remoto reservado para el tráfico de datos no orientado a conexión.

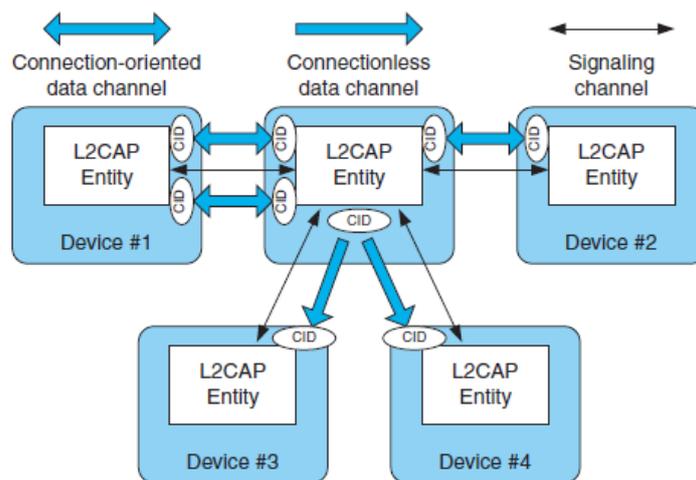


Figura 3.2.19. Ejemplo del uso y significado del campo CID.

Con respecto al modo de funcionamiento de L2CAP, este protocolo puede operar de tres formas diferentes:

- **Modo L2CAP básico.**
- **Modo control de flujo.** En este modo, en caso de pérdida no se realizan retransmisiones, sino que se detecta las PDU's perdidas y se notifican a las capas superiores.
- **Modo retransmisión.** Se caracteriza por la utilización de un temporizador que garantiza que todas las PDU's son entregadas a la entidad L2CAP par, retransmitiendo al vencimiento del mismo aquellas que fuesen necesarias. Se utiliza un mecanismo de tipo go-back-n, gracias al cual se puede simplificar el protocolo y limitar los requisitos de los buffers.

El modo L2CAP básico es el modo ejecutado por defecto, es decir, cuando el dispositivo no ha sido configurado previamente para funcionar en alguno de los otros dos.

3.3. Perfiles

Para que un dispositivo pueda utilizar la tecnología inalámbrica Bluetooth, debe saber interpretar los perfiles Bluetooth, que describen las distintas aplicaciones posibles. Estos perfiles son guías que indican los procedimientos por los que los dispositivos equipados con tecnología Bluetooth se comunican entre sí. Existe un amplio abanico de perfiles que detallan los diferentes tipos de uso y aplicaciones de la tecnología inalámbrica Bluetooth. Al seguir las directrices proporcionadas en las especificaciones Bluetooth, los desarrolladores pueden crear aplicaciones compatibles con otros dispositivos que se ajusten a este estándar.

Cada perfil incluye, como mínimo, información sobre las siguientes cuestiones:

- Dependencia de otros perfiles
- Propuestas de formato de interfaz de usuario
- Características concretas de la pila de protocolos Bluetooth utilizada por el perfil. Para realizar su función, cada perfil se sirve de ciertas opciones y parámetros en cada capa de la pila. También se puede incluir un breve resumen de los servicios requeridos si resulta necesario.

En la tabla 3.5, se recogen todos los perfiles soportados por la especificación Bluetooth v.2.1, así como los protocolos en los que se apoyan estos para hacer uso de las capas inferiores de la norma.

Perfil	Descripción
Perfil de distribución de audio avanzado (A2DP)	El perfil A2DP describe cómo transferir sonido estéreo de alta calidad de una fuente de sonido a un dispositivo receptor.
Protocolo de control de audio y vídeo (AVRCP)	El perfil AVRCP proporciona una interfaz estándar para manejar televisiones, equipos de alta fidelidad o cualquier otro equipo electrónico, y permitir así que un único control remoto, o cualquier otro tipo de mando, controle todo el equipo de audio y vídeo al que el usuario tiene acceso.
Perfil básico de imagen (BIP)	El perfil BIP establece cómo puede controlarse remotamente un dispositivo de imagen, así como la forma de enviarle órdenes de impresión y de transferencia de imágenes a un dispositivo de almacenamiento.
Perfil básico de impresión (BPP)	El perfil BPP permite enviar mensajes de texto, de correo electrónico, tarjetas de visita electrónicas e imágenes, entre otras cosas, a las impresoras disponibles dependiendo de las tareas de impresión.
Perfil de acceso RDSI común (CIP)	El perfil CIP establece cómo se deben transferir las señales RDSI a través de una conexión inalámbrica <i>Bluetooth</i> .
Perfil de telefonía inalámbrica (CTP)	El perfil CTP describe la implementación de un teléfono inalámbrico a través de un enlace inalámbrico <i>Bluetooth</i> .
Perfil de red de marcado (DUN)	El perfil DUN proporciona un acceso telefónico estándar a Internet y a otros servicios de marcado a través de una conexión <i>Bluetooth</i> .
Perfil de fax (FAX)	El perfil FAX describe cómo un dispositivo terminal puede utilizar a otro como puerta de enlace para la transmisión de faxes.
Perfil de transferencia de archivos (FTP)	El perfil FTP establece los procedimientos de exploración de carpetas y archivos de un servidor a través de un dispositivo cliente.
Perfil de distribución genérica de audio y vídeo (GAVDP)	El perfil GAVDP sienta las bases de los perfiles A2DP y VDP, pilar de los sistemas diseñados para la transmisión de sonido e imagen mediante la tecnología <i>Bluetooth</i> .
Perfil genérico de intercambio de objetos (GOEP)	El GOEP se utiliza para transferir objetos de un dispositivo a otro.
Perfil manos libres (HFP)	El perfil HFP describe cómo un dispositivo que actúa como puerta de enlace puede utilizarse para realizar y recibir llamadas a través de un dispositivo manos libres.
Perfil de sustitución de cable de copia impresa (HCRP)	El perfil HCRP describe cómo imprimir archivos mediante un enlace inalámbrico <i>Bluetooth</i> utilizando controladores en el proceso.
Perfil de auricular (HSP)	El HSP describe cómo un auricular con tecnología <i>Bluetooth</i> se comunica con otro dispositivo con tecnología <i>Bluetooth</i> .
Perfil de dispositivo de interfaz humana (HID)	El perfil HID recoge los protocolos, procedimientos y características empleados por las interfaces de usuario <i>Bluetooth</i> tales como teclados, dispositivos punteros, consolas o aparatos de control remoto.
Perfil de intercomunicador (ICP)	El perfil ICP establece cómo conectar dos teléfonos móviles con tecnología <i>Bluetooth</i> dentro la misma red sin utilizar la red telefónica pública.
Perfil de introducción de objetos (OPP)	Este perfil distingue entre servidor y cliente de introducción (push) de objetos.

Perfil de redes de área personal (PAN)	El perfil PAN describe cómo dos o más dispositivos con tecnología <i>Bluetooth</i> pueden formar una red ad hoc y cómo ese mismo mecanismo permite acceder a la red de forma remota a través de un punto de acceso.
Perfil de aplicación de descubrimiento de servicio (SDAP)	El perfil SDAP detalla cómo una aplicación debe utilizar el perfil SDP para identificar los servicios de un dispositivo remoto.
Perfil de servicio de puerto (SPP)	El perfil SPP describe cómo configurar puertos de serie y conectar dos dispositivos con tecnología <i>Bluetooth</i> .
Perfil de sincronización (SYNC)	El perfil SYNC se utiliza junto al GOEP para sincronizar los elementos del administrador de información personal (PIM), como agendas y datos de contacto, entre dispositivos con tecnología <i>Bluetooth</i> .
Perfil de distribución de vídeo (VDP)	Este perfil dicta los pasos que deben seguir los dispositivos <i>Bluetooth</i> con tecnología <i>Bluetooth</i> para la transferencia de flujos de datos de vídeo.
Protocolo	Descripción
Protocolo de control de audio y vídeo (AVCTP)	El protocolo AVCTP describe los mecanismos de transferencia para intercambiar mensajes que permitan controlar los dispositivos de audio y vídeo.
Protocolo de distribución de audio y vídeo (AVDTP)	El AVDTP detalla los procedimientos de negociación, establecimiento y transmisión del flujo de audio y vídeo.
Protocolo <i>Bluetooth</i> de encapsulación de red (BNEP)	El protocolo BNEP se utiliza para transportar protocolos de red comunes, como IPv4 o IPv6, entre los distintos medios de transmisión <i>Bluetooth</i> .
Protocolo de intercambio de Objetos (OBEX)	OBEX es un protocolo de transferencia que define los objetos de datos y el protocolo de comunicaciones que deben utilizar dos dispositivos para intercambiar objetos.
Protocolo de control de telefonía (TCP)	Este protocolo establece la señalización para el establecimiento de llamadas de voz y datos en dispositivos con tecnología <i>Bluetooth</i> .
RFCOMM con TS 07.10	El protocolo RFCOMM emula los parámetros de un cable de serie y el estado de un puerto RS-232 para transmitir datos en serie.

Tabla 3.3.1. Perfiles y protocolos soportados por la especificación 2.1 de Bluetooth.

En esta sección se procederá a desarrollar el protocolo RFCOMM exclusivamente debido a que es el utilizado en la realización del proyecto. Por este motivo, se le recomienda al lector si está interesado en conocer en detalle algún perfil o protocolo diferente a éste en mayor profundidad, acuda a la referencia [referencia SIG Bluetooth] y revise el documento correspondiente.

3.3.1. RFCOMM

El protocolo RFCOMM suministra al dispositivo Bluetooth un mecanismo de emulación de puerto serie sobre el protocolo L2CAP. Se corresponde con un protocolo de transporte sencillo que se usa para el transporte de los datos de usuario, de las señales de control de

módem y de los comandos de configuración. Se encuentra basado en la especificación TS07.10 de la ETSI, *European Telecommunications Standards Institute*, organismo que se encarga de la normalización en la industria de las telecomunicaciones.

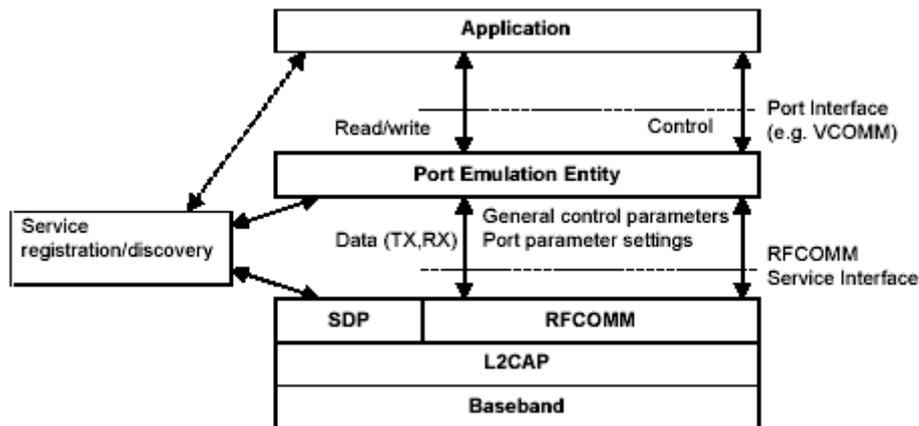


Figura 3.3.1. Modelo de referencia RFCOMM.

En la figura 3.3.1 se puede observar los elementos en los que se apoya RFCOMM. De todos ellos cabe destacar la entidad de emulación de puertos, ubicada por encima de dicho protocolo y cuya misión radica en traducir la interfaz de comunicación específica de un sistema en servicios RFCOMM. Sobre dicha capa, se apoyaría la aplicación en cuestión, la cual estaría contemplando una interfaz de comunicaciones equivalente a un puerto serie. El resto de elementos se corresponde con protocolos o niveles detallados en secciones anteriores.

Para la finalidad de RFCOMM, se requiere de dos aplicaciones ejecutándose en dispositivos diferentes que esperan que la comunicación tenga lugar a través de un cable serie, el cual resultará emulado por este protocolo. No obstante, dichas aplicaciones, al no ser conscientes de los procedimientos Bluetooth para establecer cables series emulados, pueden necesitar la ayuda de una aplicación auxiliar que utilice la especificación Bluetooth a ambos lados del enlace.

Por su parte, existen dos tipos de dispositivos básicos a los que RFCOMM debe dar servicio:

- Dispositivos que actúan como terminaciones de la comunicación, como puede ser un ordenador o una impresora.
- Dispositivos que forman parte del enlace de comunicación como resulta ser un módem.

Aunque RFCOMM no hace distinciones entre estos dos dispositivos, el uso de uno u otro terminal posee implicaciones en el protocolo, tales como el uso de tramas utilizadas exclusivamente por un tipo.

3.3.1.1. Señales de control

RFCOMM emula las 9 líneas de una interfaz RS-232. Estas quedan registradas en la siguiente tabla:

Pin	Descripción
102	Señal común
103	Transmisión (TXD)
104	Recepción (RXD)
105	Petición para envío (RTS)
106	Limpiar para enviar (CTS)
107	Conjunto de datos listos (DTS)
108	Terminal de datos listo (DTR)
109	Detección de portadora de datos (CD)
125	Indicador de llamada (RI)

Tabla 3.3.2. Líneas RS-232 emuladas en RFCOMM.

3.3.1.2. Emulación Módem-Null

Como se ha comentado anteriormente, RFCOMM está basado en TS07.10. Esta norma no distingue entre dispositivos DTE, equipo terminal de datos, y DCE, equipo de comunicación de datos, cuando se trata de transferir los estados de los circuitos que no son de datos. Para ello, lo que se hace es enviar las señales de control RS-232 como una serie de señales DTE/DCE independientes.

Señales TS 07.10	Señales de control RS-232 correspondientes
RTC	DSR, DTR
RTR	RTS, CTS
IC	RI
DV	DCD

Tabla 3.3.3. Correspondencia de las señales de control recogidas en la norma TS07.10 y las señales de control RS-232.

La forma en la que TS07.10 transfiere las señales de control RS-232 es creando un enlace modem-null implícito cuando dos dispositivos del mismo tipo se conectan entre sí. Este sistema previsto por RFCOMM deberá funcionar en la mayoría de las situaciones posibles.

3.3.1.3. Puerto serie emulado

Este protocolo soporta hasta 60 conexiones simultáneas entre dos dispositivos Bluetooth. No obstante, este número puede variar según la implementación específica del fabricante. Un identificador de enlace de datos de conexión (DLCI) identifica una conexión permanente entre un cliente y un servidor de aplicaciones. El DLCI está representado por 6 bits, pero su rango de valores utilizables oscila entre 2 y 61. El identificador de enlaces es único dentro de una sesión RFCOMM entre dos dispositivos.

Para tener en cuenta el hecho de que tanto el cliente como servidor de aplicaciones pueden residir en ambos lados de una sesión RFCOMM, con clientes en ambos lados pudiendo realizar conexiones independientes entre sí, el espacio de valores DLCI se divide entre los dos dispositivos que se comunican mediante el concepto de servidor RFCOMM canales.

Si un dispositivo Bluetooth soporta múltiples puertos series emulados y se les permite a las conexiones tener terminaciones en los diferentes dispositivos, la entidad RFCOMM debe ser capaz de ejecutar múltiples sesiones TS07.10. Esta tarea se lleva a cabo mediante el multiplexor de sesiones. Para ello, cada sesión es multiplexada utilizando su propio identificador de canal, CID. La capacidad de ejecutar múltiples sesiones es una característica opcional del protocolo RFCOMM.