

Bluetooth

Iker Costa Fernández de Luco
Asier Núñez Domingo

Índice

Introducción

Evolución histórica

Topologías de comunicación

Especificaciones

Seguridad

Diálogos

Introducción

Origen

Grupo de trabajo IEEE 802.15

Contexto dentro de las tecnologías WPAN

Objetivos



Introducción

- Wireless Personal Area Network (WPAN).
- También conocido como IEEE 802.15.
- Interesante para dispositivos pequeños (IoT).
- Permite interconexión de dispositivos a 10 metros.
- Banda 2,4 GHz.
- El canal permanece abierto.

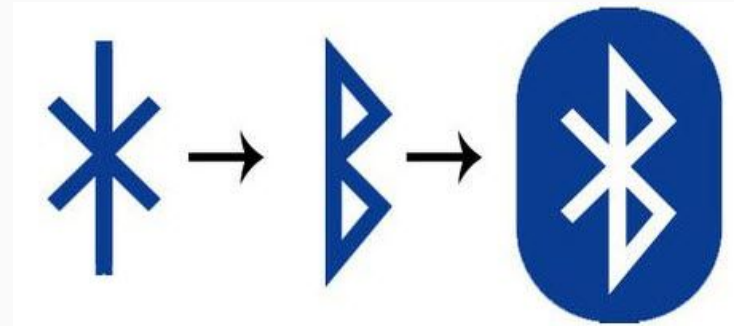
Origen

- Estudio de 1994 de Ericsson.
- Objetivo: eliminar el uso de cables entre dispositivos.
- Resultado: MC Link.
- En 1998 se crea un grupo de especial interés (SIG) formado por:
 - Ericsson.
 - Nokia.
 - IBM.
 - Intel.
 - Toshiba



Origen

- Nombre proveniente de un Rey danés del siglo X:
 - Harald Blatand (Harold Bluetooth).
 - Unificó los reinos de Dinamarca y Noruega
- Asimilaron el Bluetooth con esa unificación.
- 2002 -> Primera versión de Bluetooth.



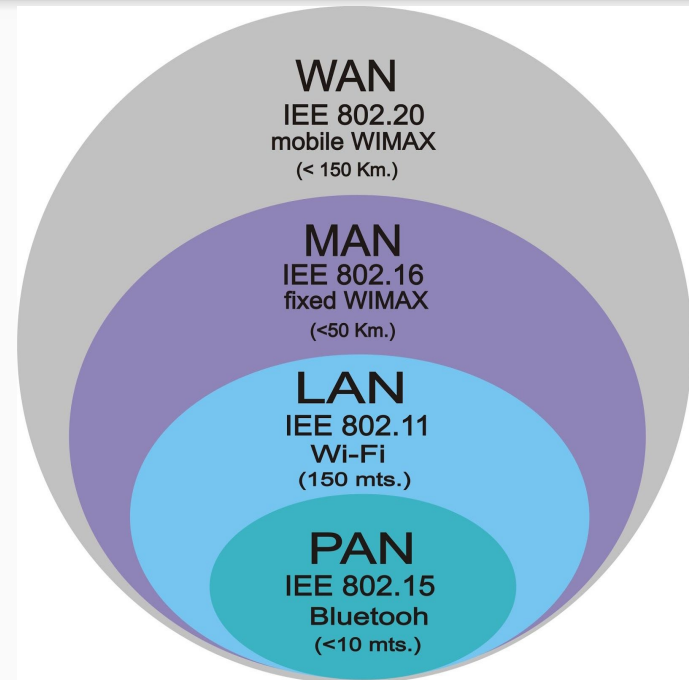
IEEE 802.15

- Estándar de las WPAN.
- Diferentes subgrupos:
 - Primeras WPAN → 802.15.1
 - Alta velocidad y UWB → 802.15.3
 - Baja velocidad (zigbee) → 802.15.4



Tecnologías WPAN

- Corto alcance.
- Sin (casi) infraestructura.
- Dispositivos pequeños.
- Bajo consumo.
- Bajo coste.
- Poca complejidad.
- Velocidades bajas.



Objetivos

- Permitir comunicación sencilla entre dispositivos.
- Evitar cables.
- Crear redes pequeñas inalámbricas.
- Reducir consumo.
- Impulsar redes de área personal.
- Interoperabilidad.
- Tecnología de bajo coste.



Evolución histórica

Histórico de versiones y características generales

Mejoras entre versiones consecutivas

Histórico de Versiones:

Características Generales

VERSIÓN	1.0	2.0	3.0	4.0	5.0	5.1	5.2
Rango (m)	10	30	30	60	240	240	240
Velocidad (Mbps)	0,732	2,1	24	24	50	50	50
Basic Rate BR	SI	SI	SI	SI	SI	SI	SI
Enhanced Data Rate EDR	NO	SI	SI	SI	SI	SI	SI
High Speed HS	NO	NO	SI	SI	SI	SI	SI
Low Energy LE	NO	NO	NO	SI	SI	SI	SI

Comparación entre versiones – V1y V2

- Triplica alcance.
- Triplica tasa de transferencia.
- Enhanced Data Rate – EDR.
- Conexión sin PIN (V2.1).

Comparación entre versiones – V2 y V3

- Mismo rango.
- Tasa de transferencia 11 veces mayor.
- High Speed – HS.



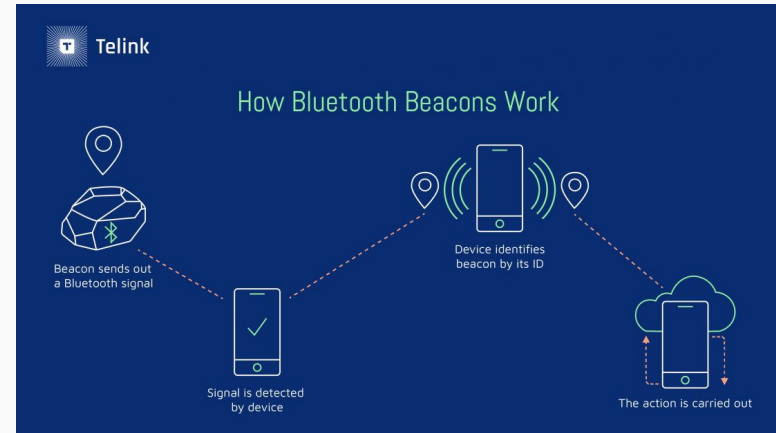
Comparación entre versiones – V3 y V4

- Duplica alcance.
- Mantiene tasa de transferencia.
- Bluetooth Low Energy.
- El bajo consumo permite su utilización en dispositivos más pequeños.
- IoT al no depender de intermediarios (V4.1).
- Internet mediante IPv6 (V4.2)



Comparación entre versiones – V4 y V5

- Cuadriplica el alcance.
- Duplica la tasa de transferencia.
- Pensado en IoT por su bajo consumo.
- Mejoras para detectar la ubicación y dirección (V5.1).



Topologías de comunicación

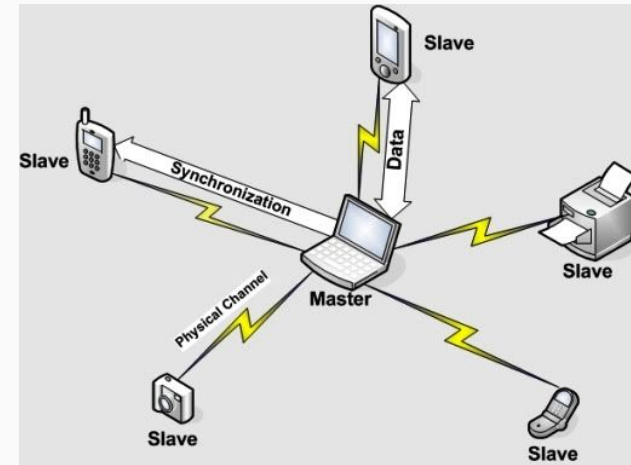
Piconet

Scatternet



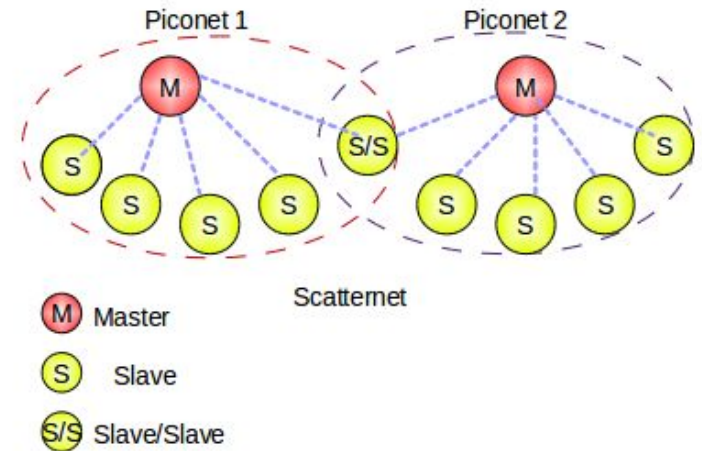
Piconet

- Conjunto de dispositivos que se pueden comunicar entre sí.
- Sin necesidad de infraestructura.
- Maestro+esclavos (cualquier dispositivo puede ser maestro o esclavo).
- Intercambian información a través del maestro.
- Cada piconet dispone de todo el ancho de banda.
- Secuencia aleatoria de salto de frecuencia.



Scatternet

- Cuando un dispositivo pertenece a varias redes Piconet a la vez, mediante TDM→ Scatternet.
- Configuración más flexible.
- Un mismo dispositivo solo puede ser maestro de una red en un momento.
- No implica encaminamiento entre redes.
- Depende de protocolos de capas superiores.
- No existe sincronización entre las Piconet.

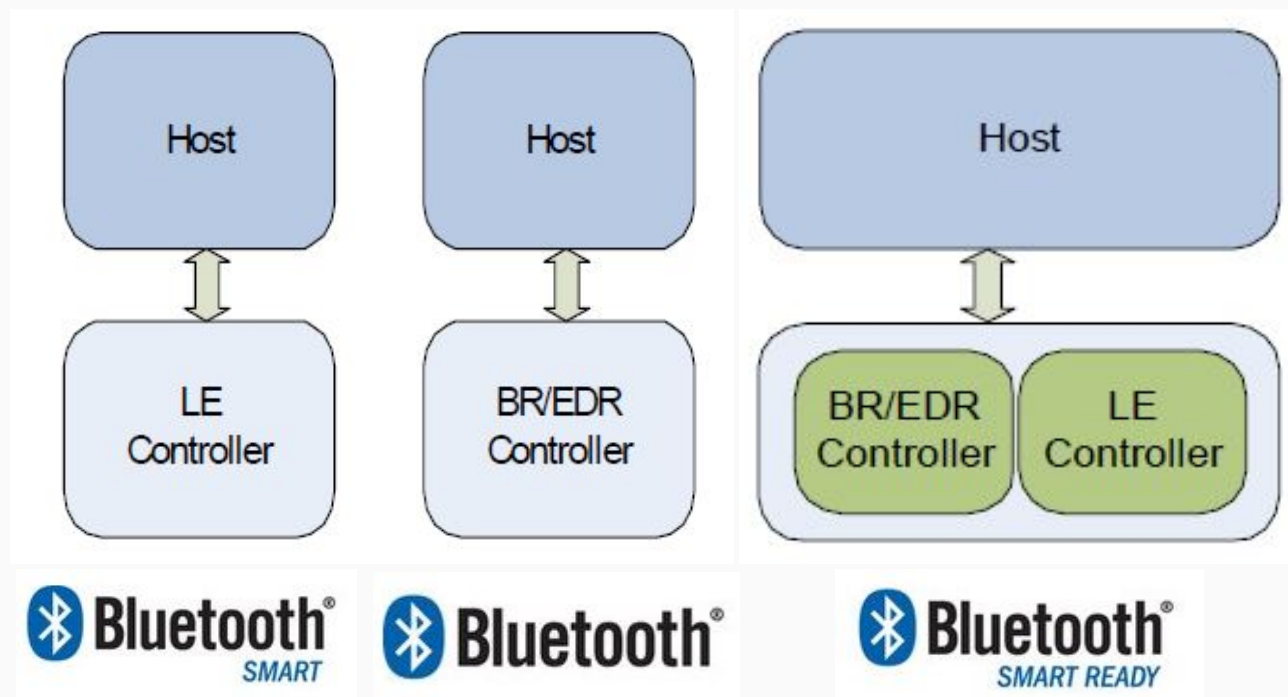


Especificaciones

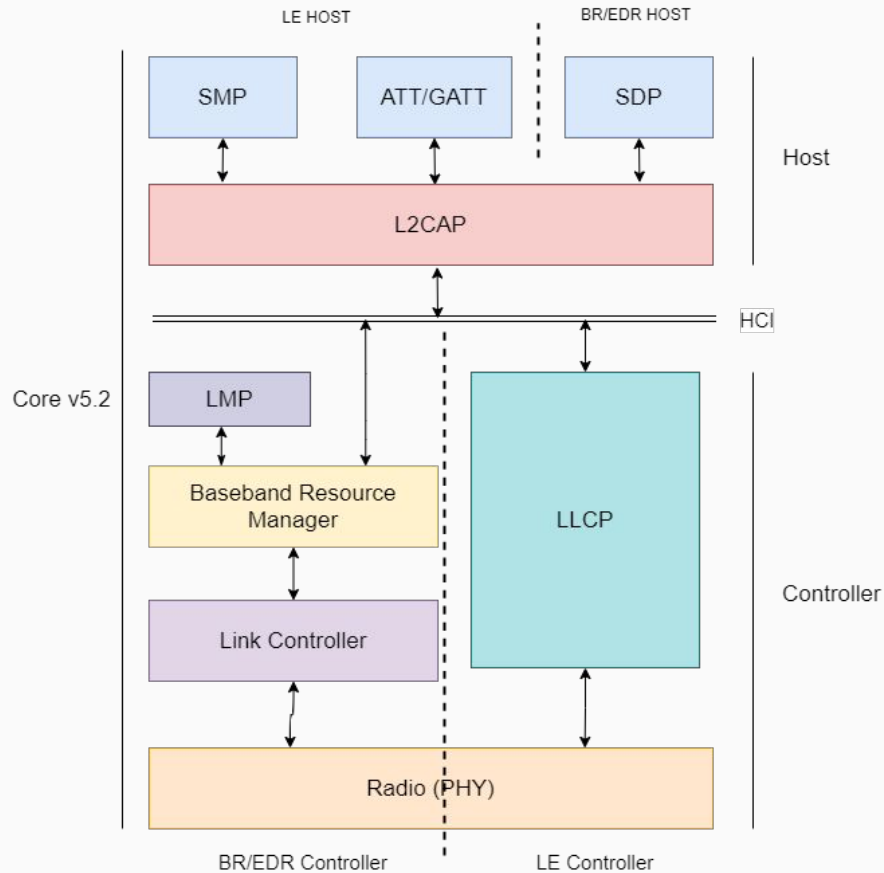
Especificación core v5.2

Especificación de perfiles

Especificación core v5.2

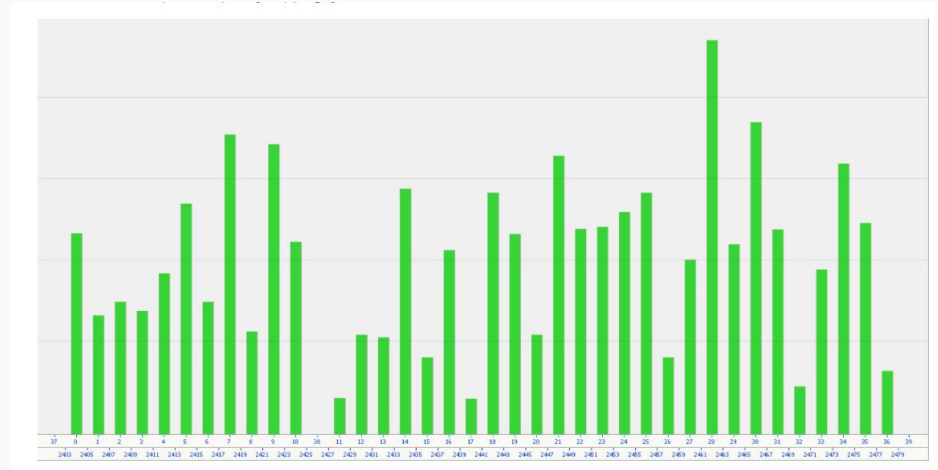


Especificación Core v5.2



Frequency Hopping

- La comunicación se llevará a cabo a través de una serie de canales de la banda ISM
- Cada canal se selecciona de un conjunto de canales usando *Channel Selection Algorithm*.
- El dispositivo primario mantiene un *mapa de canales* que los clasifica en *usados* y *no usados*.
- El *mapa de canales* se comparte al dispositivo secundario para que pueda seguir la serie de canales.



Controlador BR/EDR

BR/EDR Radio

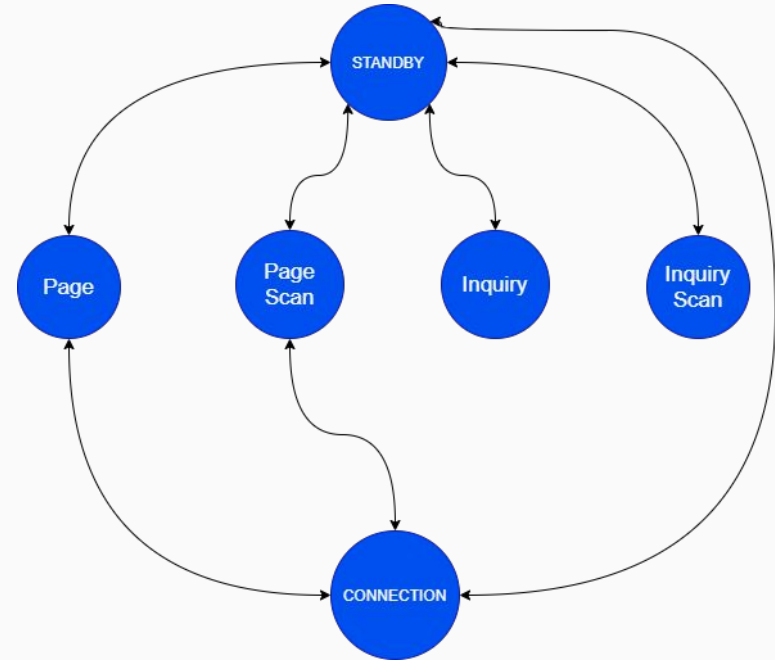
- Banda de frecuencia 2.4 GHz ISM. →
- Frequency Hopping: combatir interferencias.
- Tres clases de transmisores →
- Modulaciones:
 - Basic Rate: GFSK (Gaussian Frequency Shift Keying)
 - Enhanced Data Rate: PSK (Phase Shift Keying)
- Time Division Duplex TDD: el canal se divide en slots de cierta duración, en cada slot sólo transmite un dispositivo.

Regulatory Range	RF Channels
2.400-2.4835 GHz	$f=2402+k$ MHz, $k=0,\dots,78$

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power ¹	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	$P_{min} < +4$ dBm to P_{max} Optional: P_{min}^2 to P_{max}
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: P_{min}^2 to P_{max}
3	1 mW (0 dBm)	N/A	N/A	Optional: P_{min}^2 to P_{max}

BR/EDR Link Controller

- Indica en qué estado se encuentra el controlador Bluetooth BR/EDR .
- El cambio entre estados se realiza a través de:
 - Comandos de la función LMP.
 - Por información que tiene el propio Link Controller.

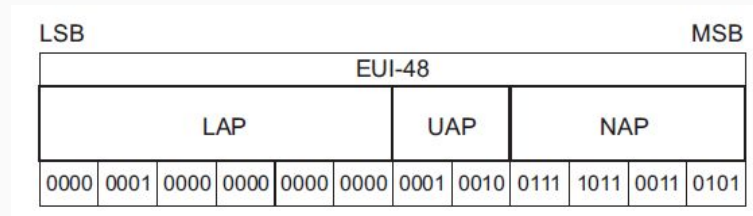


Especificación Core v5.2

Estado	Descripción	Eventos de entrada	Eventos de salida
STANDBY	Estado por defecto. Low power mode.	Liberación de piconet. Dejar de escuchar o realizar solicitudes de: <ul style="list-style-type: none">- Conexión (Page)- Descubrimiento (Inquiry)	Escuchar o realizar solicitudes de: <ul style="list-style-type: none">- Conexión (Page)- Descubrimiento (Inquiry)
Page	Estado de realización de solicitud de conexión a un esclavo.	Liberación de piconet. Comando de la función LMP.	Establecimiento de piconet. Comando de la función LMP.
Page scan	Estado de escucha de solicitud de conexión de un maestro.	Liberación de piconet. Comando de la función LMP	Establecimiento de piconet. Comando de la función LMP.
Inquiry scan	Estado de escucha de solicitudes de descubrimiento de dispositivos.	Comando de la función LMP.	Timer.
Inquiry	Estado de realización de solicitudes de descubrimiento de dispositivos.	Comando de la función LMP.	Timer.
CONNECTION	Piconet establecida.	Establecimiento de piconet.	Liberación de piconet.

BR/EDR Baseband Resource Manager

- Nivel de enlace.
- Define el control de acceso al medio:
 - El dispositivo maestro transmite en slots pares.
 - El dispositivo esclavo transmite en slots impares.
- Define las direcciones de los dispositivos Bluetooth:
 - Cada dispositivo tiene una dirección de 48 bits única (BD_ADDR).
 - Se obtienen a través de *IEEE Registration Authority*.

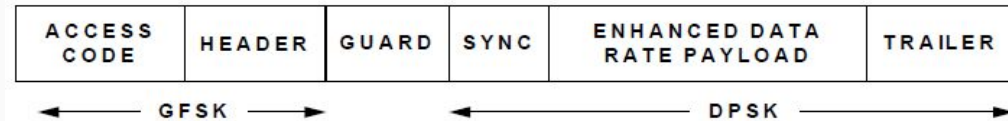


BR/EDR Baseband Resource Manager

- Convierte flujos de bits en tramas.
 - Trama en modo BR



- Trama en modo EDR



BR/EDR Baseband Resource Manager

- Access code:
 - 72 bits.
 - Utilizado para sincronización.
 - Robusto y resistente a la interferencia.

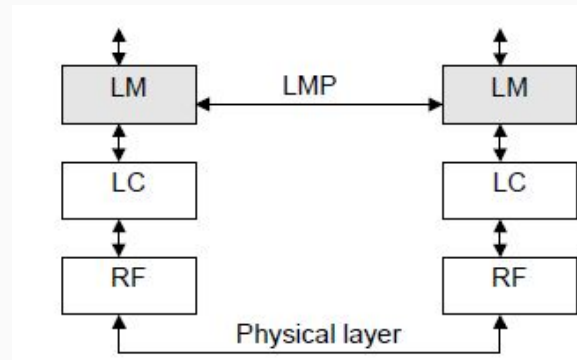
Access code	Descripción	Deriva de
Channel Access Code CAC	En mensajes con piconet establecida.	LAP del maestro
Device Access Code DAC	En mensajes Page o en su respuesta.	LAP del dispositivo destino del Page
Device Inquiry Access Code DIAC	En mensajes Inquiry o en su respuesta.	LAP del dispositivo destino del mensaje Inquiry
Group Inquiry Access Code GIAC	En mensajes grupales Inquiry o en su respuesta.	Fijo: 0x9E8B33

BR/EDR Baseband Resource Manager

- Header:
 - LT_ADDR: 3 bits. Dirección de transporte lógico.
 - Type: 4 bits. Tipo del paquete y slots que ocupa.
 - Flow: 1 bit. Control de flujo. STOP = 0, GO = 1
 - ARQN: 1 bit de reconocimiento de paquetes. 1 ACK 0 NACK.
 - SEQN: 1 bit que se va invirtiendo para evitar retransmisiones en el receptor.
 - HEC: 8 bits para comprobar la integridad de la cabecera.
- Guard: Periodo de guarda que permite la transición entre modulaciones.
- Sync y Trailer : Sincronización

BR/EDR Link Manager Protocol

- Define los siguientes puntos:
 - Establecimiento y liberación de una conexión entre dos dispositivos.
 - Gestión del enlace creado entre dos dispositivos.
 - Seguridad: confidencialidad y autenticación.
- Para el establecimiento, gestión, liberación y seguridad de una conexión se intercambian mensajes entre ambos dispositivos a nivel LMP.



BR/EDR Link Manager Protocol



- LMP funciona en base a transacciones, modelo petición/respuesta.
- Formato de los mensajes:



- El OpCode puede ser de 7 bits o 15 bits. Indica el tipo de operación que se desea realizar, por ejemplo:
 - Enviar el mapa de canales
 - Solicitud de conexión
 - Liberación de conexión
 - ...

Controlador LE

LE Radio

- Banda de frecuencia 2.4 GHz ISM. 
- Frequency Hopping: combatir interferencias.
- Cuatro clases de transmisores 
- Modulación GFSK (Gaussian Frequency Shift Keying)
- Time Division Duplex TDD: el canal se divide en slots de cierta duración, en cada slot sólo transmite un dispositivo.

Regulatory Range	RF Channels
2.400-2.4835 GHz	$f=2402+k*2$ MHz, $k=0, \dots, 39$

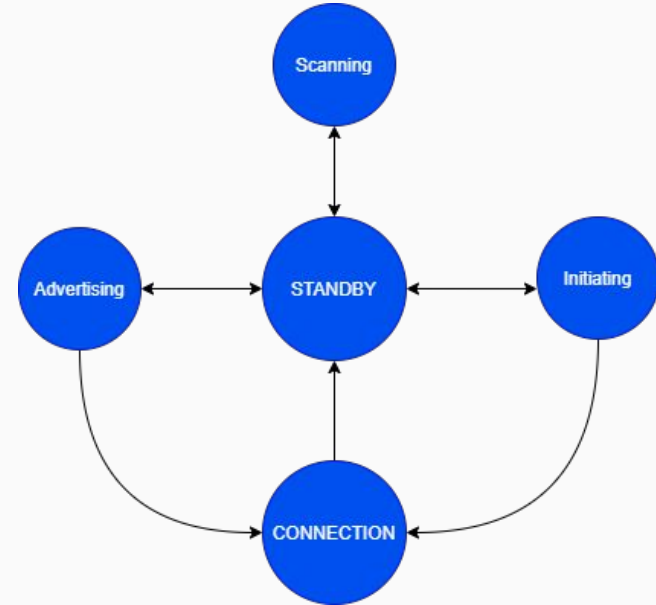
Power Class	Maximum Output Power (P_{\max})	Minimum Output Power ¹
1	100 mW (+20 dBm)	10 mW (+10 dBm)
1.5	10 mW (+10 dBm)	0.01 mW (-20 dBm)
2	2.5 mW (+4 dBm)	0.01 mW (-20 dBm)
3	1 mW (0 dBm)	0.01 mW (-20 dBm)

LE Link Layer Controller Protocol LLCP Funciones

- Nivel de enlace.
- Define el control de acceso al medio:
 - El dispositivo maestro transmite en slots pares.
 - El dispositivo esclavo transmite en slots impares.
- Define las direcciones de los dispositivos Bluetooth:
 - Una dirección pública de 48 bits, en acorde a *IEEE Registration Authority*.
 - Una dirección aleatoria de 48 bits:
 - Estática: es generada en cada ciclo de encendido del dispositivo.
 - Privada:
 - Sin resolución: ningún dispositivo puede comunicarse con él.
 - Con resolución: se genera a través de una clave. Sólomente un dispositivo de confianza podría comunicarse con él.
- Podría tener sólomente un tipo de dirección o ambas.

LE Link Layer Controller Protocol LLCP Estados

- Indica en qué estado se encuentra el controlador Bluetooth LE.
- El cambio de estados se hace a través de:
 - Comandos enviados por HCI.
 - Información propia de LLCP.



Especificación Core v5.2

Estado	Descripción	Eventos de entrada	Eventos de salida
STANDBY	Estado por defecto.	Liberación de piconet.	Comando de LMP: <ul style="list-style-type: none">- Scanning- Advertising- Initiating
Scanning	El dispositivo se encuentra escaneando dispositivos cercanos.	Comando de HCI	Timer.
Advertising	El dispositivo se encuentra transmitiendo paquetes advertising y escuchando solicitudes de conexión.	Comando de HCI	Establecimiento piconet.
Initiating	El dispositivo se encuentra escuchando paquetes advertising de dispositivos en concreto para iniciar conexiones hacia ellos.	Comando de HCI	Establecimiento piconet.
CONNECTION	Piconet establecida.	Establecimiento de piconet <ul style="list-style-type: none">- Rol maestro si viene de Initiating- Rol esclavo si viene de Advertising	Liberación de piconet

LE Link Layer Controller Protocol LLCP Formato de mensajes en el aire

- Preamble: sincronización entre dispositivos.
- Access-Address indica el tipo de paquete:
 - advertising: 0x8E89BED6
 - Inicio de conexión
 - Solicitud de escaneo
 - Envío del mapa de canales
 - ...
- PDU: datos. Cada Access-Address tiene un formato de PDU diferente.
- CRC: Mecanismo de detección de errores. Aplicado a la PDU.

Preamble (1 or 2 octets)	Access-Address (4 octets)	PDU (2-258 octets)	CRC (3 octets)
-----------------------------	------------------------------	-----------------------	-------------------

HCI

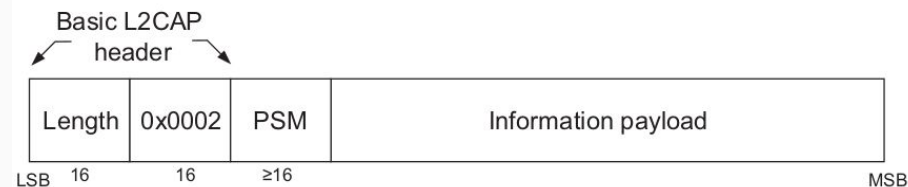
HCI

- Provee una interfaz uniforme al host para acceder a los servicios que le ofrecen los controladores Bluetooth.
- La interfaz consta de:
 - Comandos hacia los controladores BR/EDR y LE:
 - Establecer conexión
 - Finalizar conexión
 - Escanear dispositivos
 - ...
 - Eventos: indican al host el resultado del comando enviado al controlador.
 - Conexión establecida
 - Desconexión completada
 - ...

Host

Logical Link Control and Adaptation Layer Protocol L2CAP

- Ofrece a protocolos superiores servicios de datos orientados a conexión y no orientados a conexión.



- L2CAP tiene la capacidad de:
 - Multiplexación de protocolos.
 - Segmentación y reensamblado. Máxima SDU: 64 KB.
 - Control de flujo y retransmisión de paquetes.
 - Canales L2CAP: multiplexados sobre uno o más enlaces banda base. Se identifican por el campo CID en el paquete L2CAP.

Service Discovery Protocol (Host BR/EDR)

- Ofrece a protocolos superiores que servicios hay disponibles en su entorno.

Attribute Protocol ATT (Host LE)

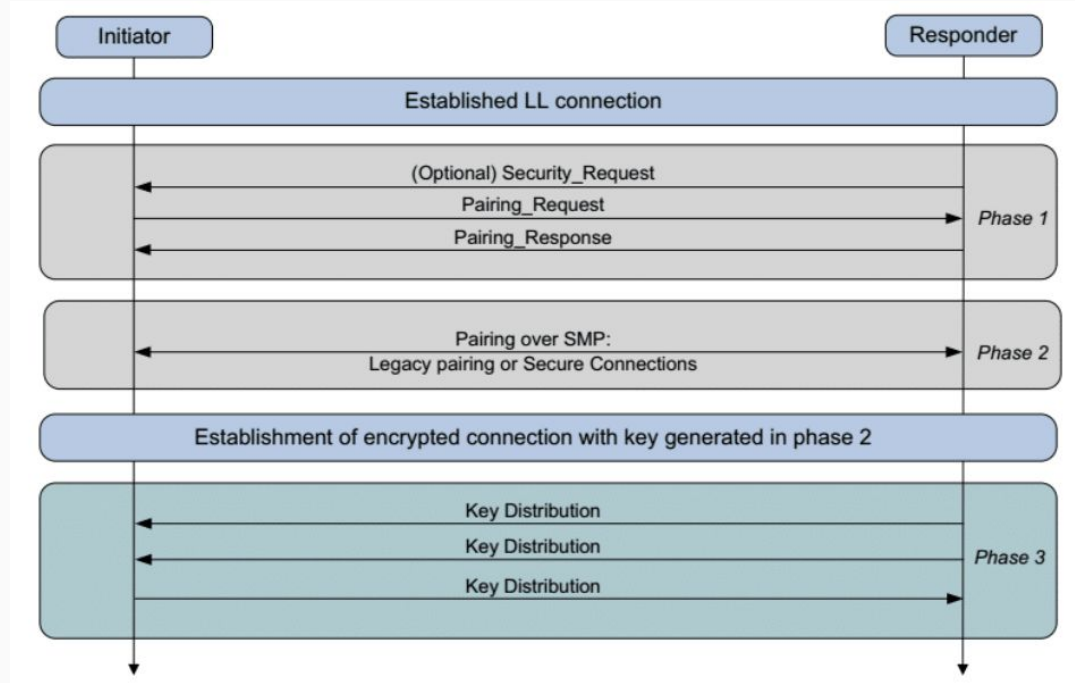
- Permite a un dispositivo con el rol de servidor exponer una serie de atributos y sus valores a otro dispositivo con el rol de cliente.
 - Atributo, definido por un UUID 128 bits
 - Valor 16 bits
 - Permisos (no se puede acceder)

Generic Attribute Protocol GATT (Host LE)

- Opera sobre ATT. Define procedimientos, formatos de servicios y sus características. Permite descubrir, escribir, leer y notificar las características de un servicio.

Security Manager Protocol SMP (LE Host)

- Define métodos emparejamiento y distribución de claves en dispositivos LE o BR/EDR/LE
- Claves AES-128-bit para cifrar datos.

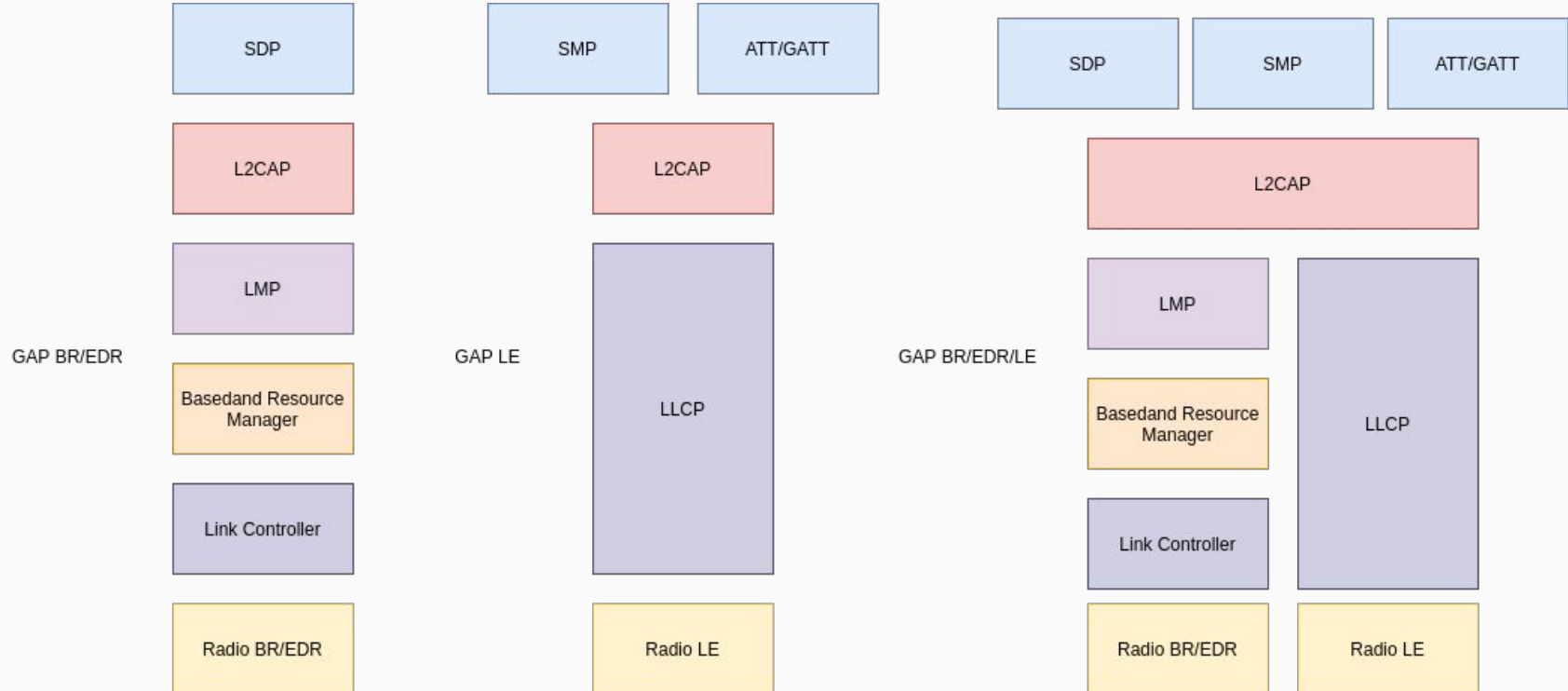


Especificación de perfiles

Especificación de perfiles

- Un perfil está definido como un conjunto de protocolos y procedimientos que se deben utilizar para una determinada aplicación.
- Permite a los fabricantes de equipos no implementar todos los protocolos en sus dispositivos.
- Garantizan la interoperabilidad entre dispositivos con los mismos perfiles.
- Pueden existir perfiles que dependan de otros perfiles.
- Existe un perfil general que sí deben implementar los dispositivos: GAP.
 - Es la base del resto de los perfiles.
 - Está formado por los protocolos de la especificación Core.

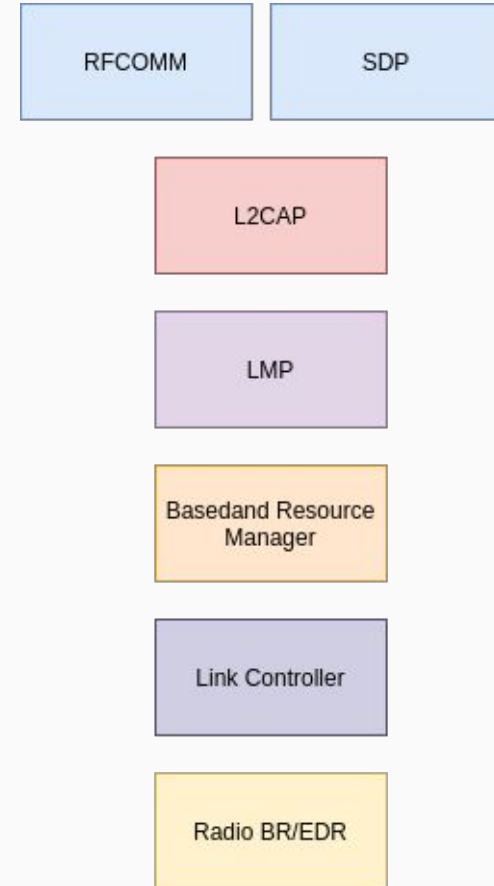
Generic Access Profile GAP



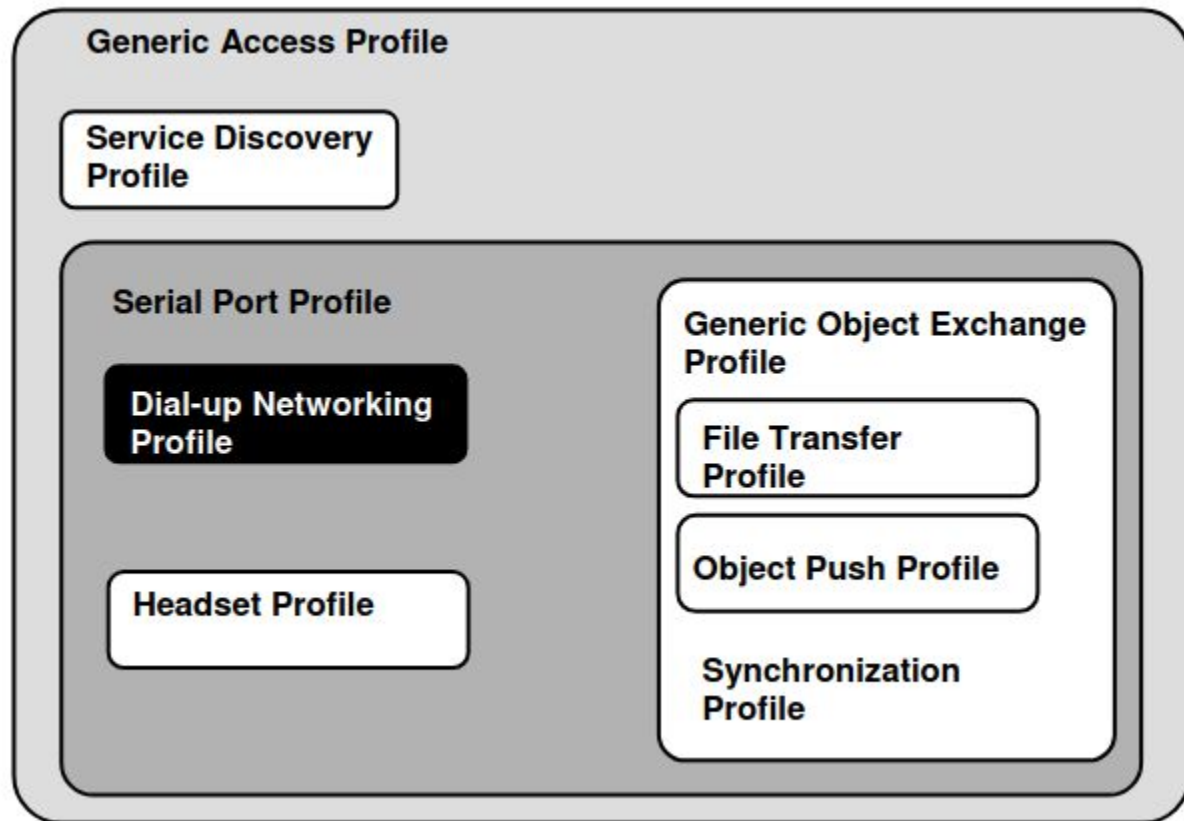
Especificación de perfiles

RFCOMM

- No está en la especificación Core desde Bluetooth v1.2.
- Protocolo que trabaja sobre L2CAP.
- Se utiliza en multitud de perfiles.
- Emula hasta nueve puertos serie RS-232.
- Permite hasta 60 conexiones simultáneas entre dos dispositivos Bluetooth.



Especificación de perfiles



Seguridad

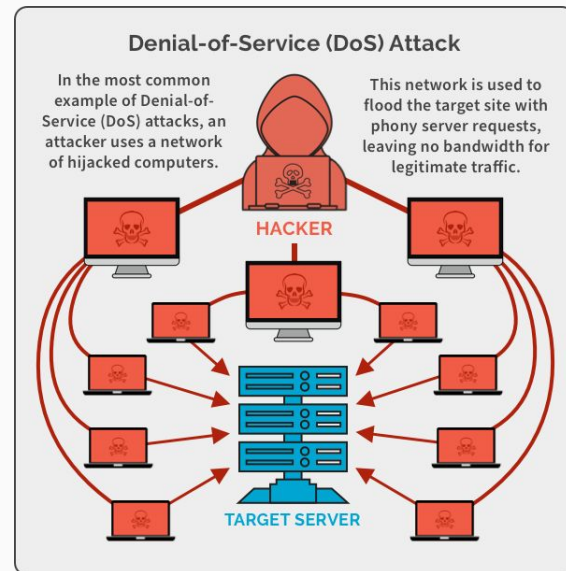
Amenazas

Modos

Medidas de seguridad

Amenazas

- Los dispositivos cercanos pueden sufrir los siguientes ataques entre otros si conocemos sus servicios:
 - Bluejacking.
 - Bluesnarfing.
 - Bluebugging.
 - DoS.
 - BlueBorne.
 - CVE-2018-5383.



Bluejacking

- Acción molesta o maliciosa.
- Spamear a una víctima.
- No hay robo de información.
- Se puede realizar de forma masiva.

Bluesnarfing

- Aprovecha vulnerabilidades conocidas.
- Varía en función de la versión de Bluetooth.
- Hay robo de información.

DoS

- El atacante envía múltiples solicitudes de emparejamiento.
- Inutiliza la interfaz Bluetooth.
- Paralización temporal del dispositivo.
- Aumento consumo de la batería.

BlueBorne

- Conjunto de exploits.
- Se aprovecha de un conjunto de vulnerabilidades de Bluetooth Network Encapsulation Protocol.
- Permite vulnerar las conexiones de la mayoría de dispositivos.

CVE-2018-5383

- Permite:
 - Interceptar.
 - Controlar.
 - Manipular.
- Requiere la inyección de una clave pública inválida durante el intercambio de claves.

Bluebugging

- Se aprovecha de los bugs de autenticación.
- Ejecuta comando AT en el dispositivo.
- Permite robar información.
- Controla el dispositivo totalmente.

Modos

- 4 modos de seguridad.
- De menos seguro a más seguro.



Modo 1 - No seguro

- Sin seguridad.
- Dispositivos indiscriminados → no previenen conexiones.

Modo 2 - Seguridad a Nivel de Servicio

- Antes de establecer canal lógico.
- Gestor de seguridad local.
- Controla acceso a servicios específicos.

Modo 3 - Seguridad a Nivel de Enlace

- Antes de establecer el enlace físico.
- Requiere:
 - Autenticación en todas las conexiones.
 - Encriptación en todas las conexiones.

Modo 4 - Seguridad después de establecimiento

- Después de establecer enlace lógico y físico.
- Utiliza Secure Simple Pairing (SSP).
- Obligatorio a partir de v2.1.
- Secure connections a partir de v4.1:
 - Actualiza algoritmos.
 - Proporciona integridad.

Medidas de Seguridad

- Emparejamiento.
- Autenticación.
- Confidencialidad.
- Autorización.

Emparejamiento

- Clave secreta y simétrica.
- 4 modelos de comparación de clave:
 - Comparación numérica.
 - Introducción de contraseña, por indicación del otro dispositivo.
 - Just works
 - Fuera de Banda (OOB) → NFC por ejemplo.



Type the following code into your device

This will verify that you are connecting to the correct device.

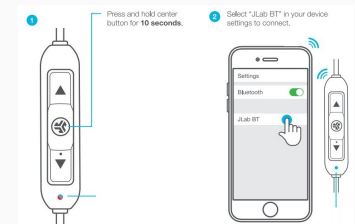
476232



SAMSUNG Keyboard

Note:

After you type this code, you might need to press Enter, OK, or a similar button on your device.



Autenticación

- Autenticación por retos.
- A envía un reto a B.
- A y B ejecutan un algoritmo para resolverlo.
- B envía la respuesta firmada a A (SRES).
- Autenticación exitosa si las dos respuestas SRES coinciden.



Confidencialidad

- Para evitar escuchas en la comunicación.
- El algoritmo de encriptación varía según la versión de Bluetooth.
- Para generar la clave de encriptación se usan:
 - Clave de enlace (emparejamiento).
 - Authenticated Ciphering Offset - ACO (autenticación).



Autorización

- Niveles de confianza (¿dispositivo de confianza?).
- Niveles de seguridad.
- Nivel 0 → Sin protección MITM, encriptación e interacción de usuario.
- Nivel 1 → Sin protección MITM ni encriptación, interacción mínima.
- Nivel 2 → Solo encriptación.
- Nivel 3 → Protección MITM y encriptación, interacción aceptable.

Problemas de seguridad

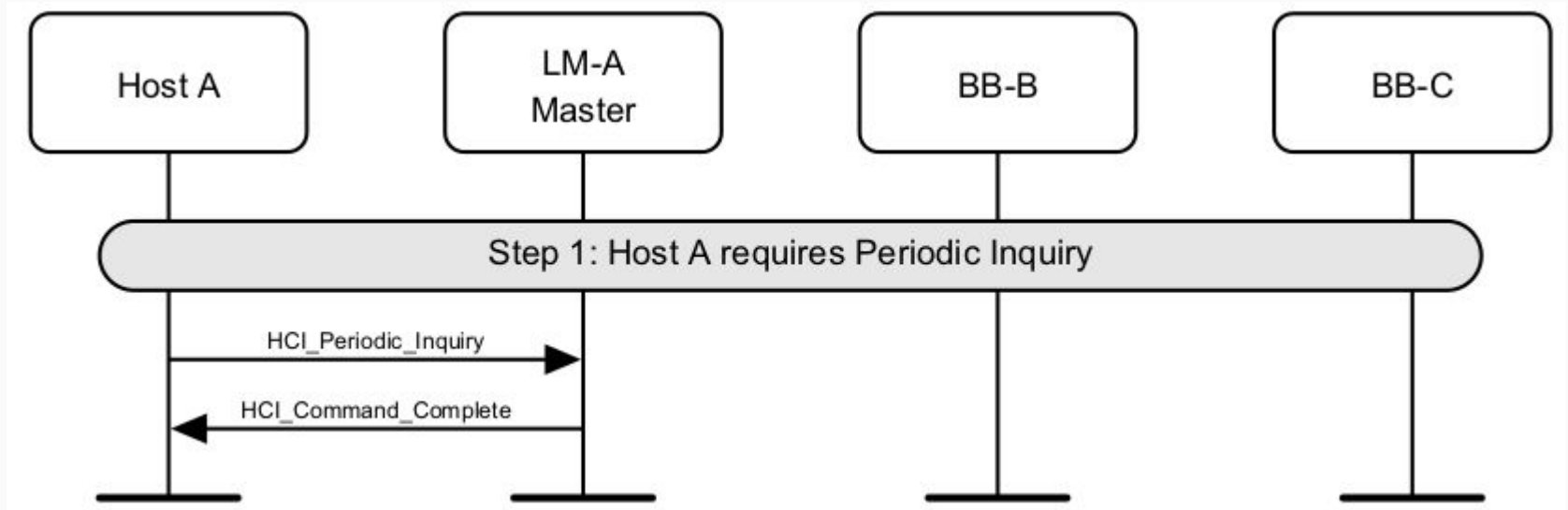
- Solo autenticación de dispositivos, no usuarios.
- Sin límite de intentos en la autenticación.
- Los retos son vulnerables a ataques MITM.
- Seguridad limitada (no hay registro por ejemplo).
- Compatibilidad entre versiones implica menor seguridad.

Diálogos

Descubrimiento de dispositivos

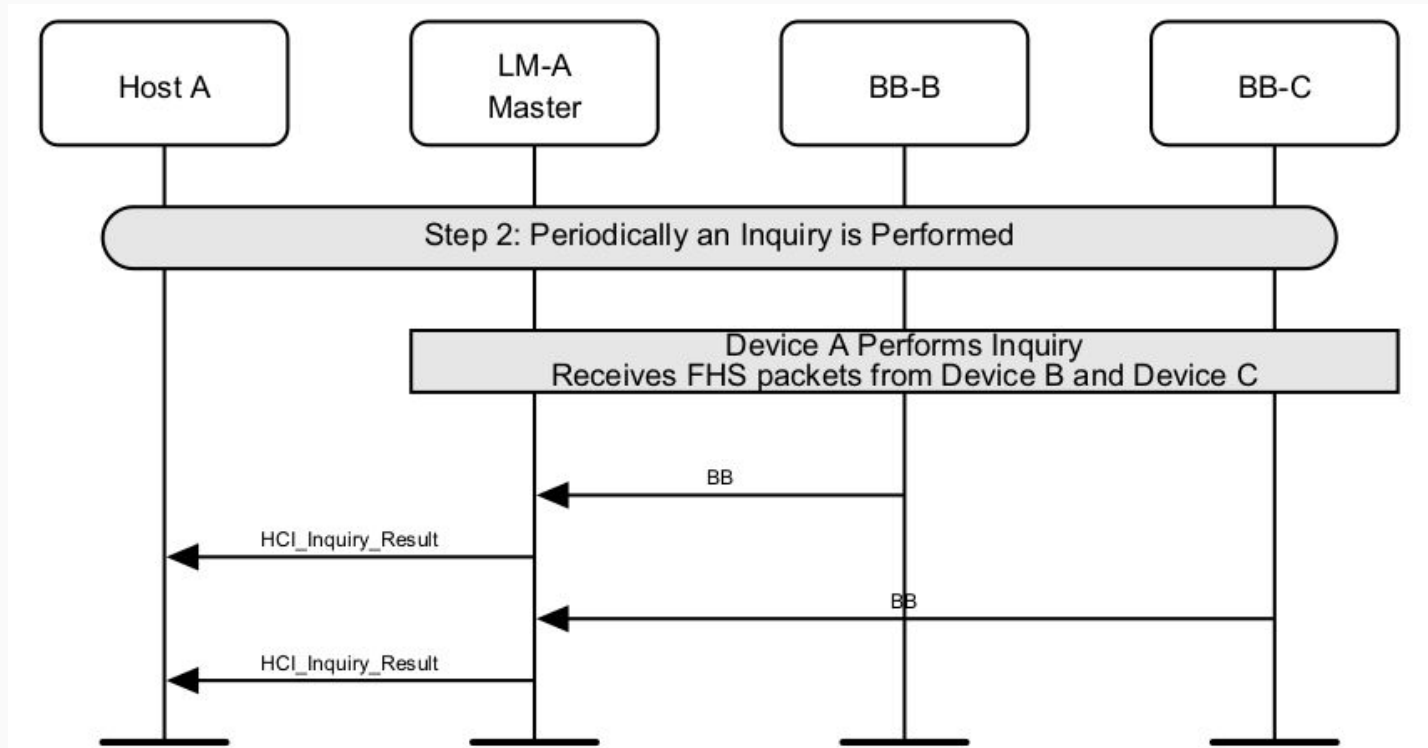
Establecimiento y liberación de conexión entre dispositivos

Bluetooth BR/EDR Procedimiento de escaneo



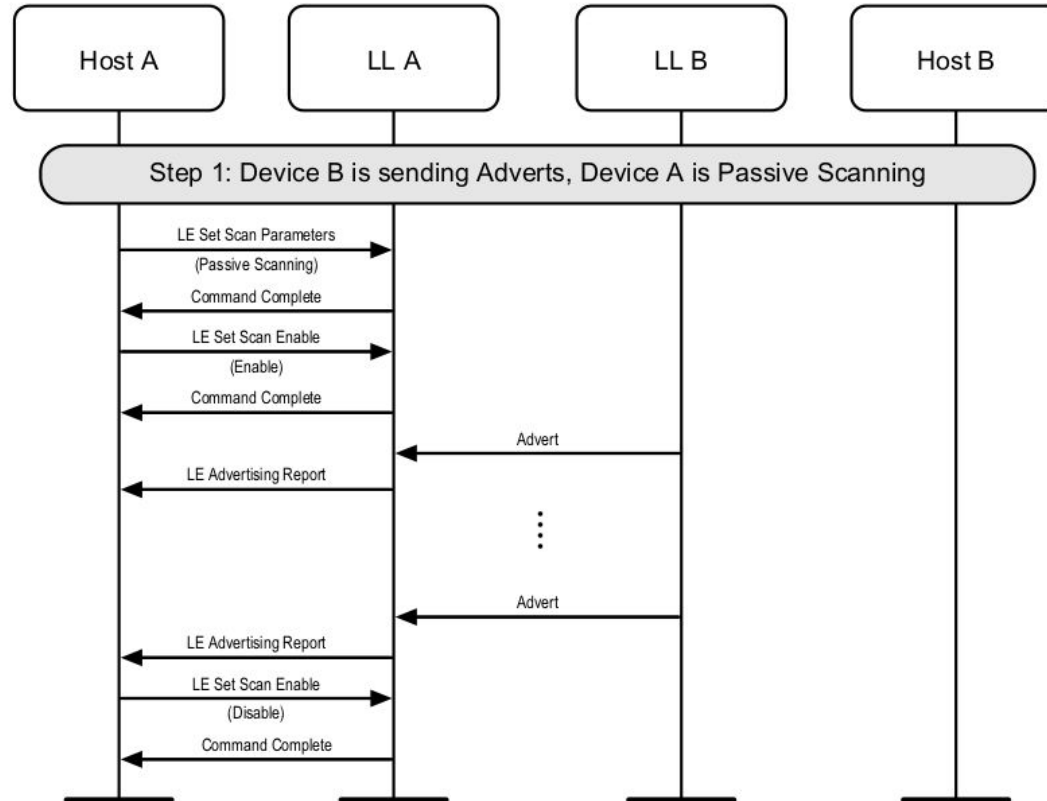
Descubrimiento de dispositivos

Bluetooth BR/EDR Procedimiento de escaneo



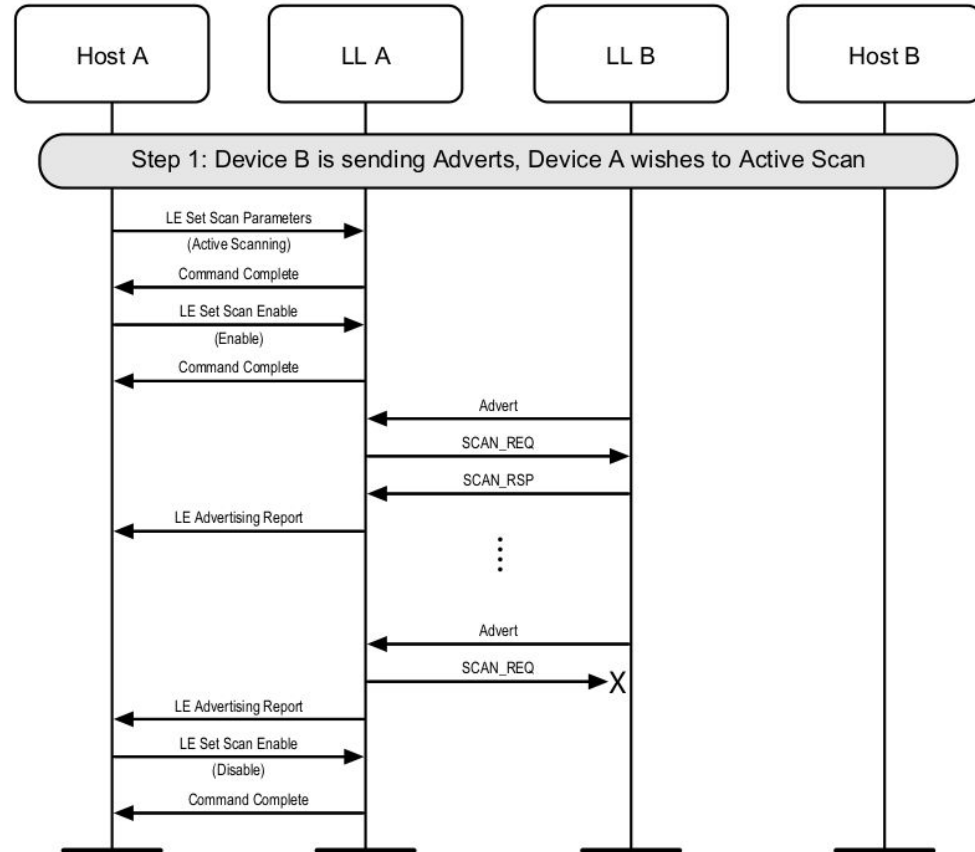
Descubrimiento de dispositivos

Bluetooth LE Escaneo pasivo



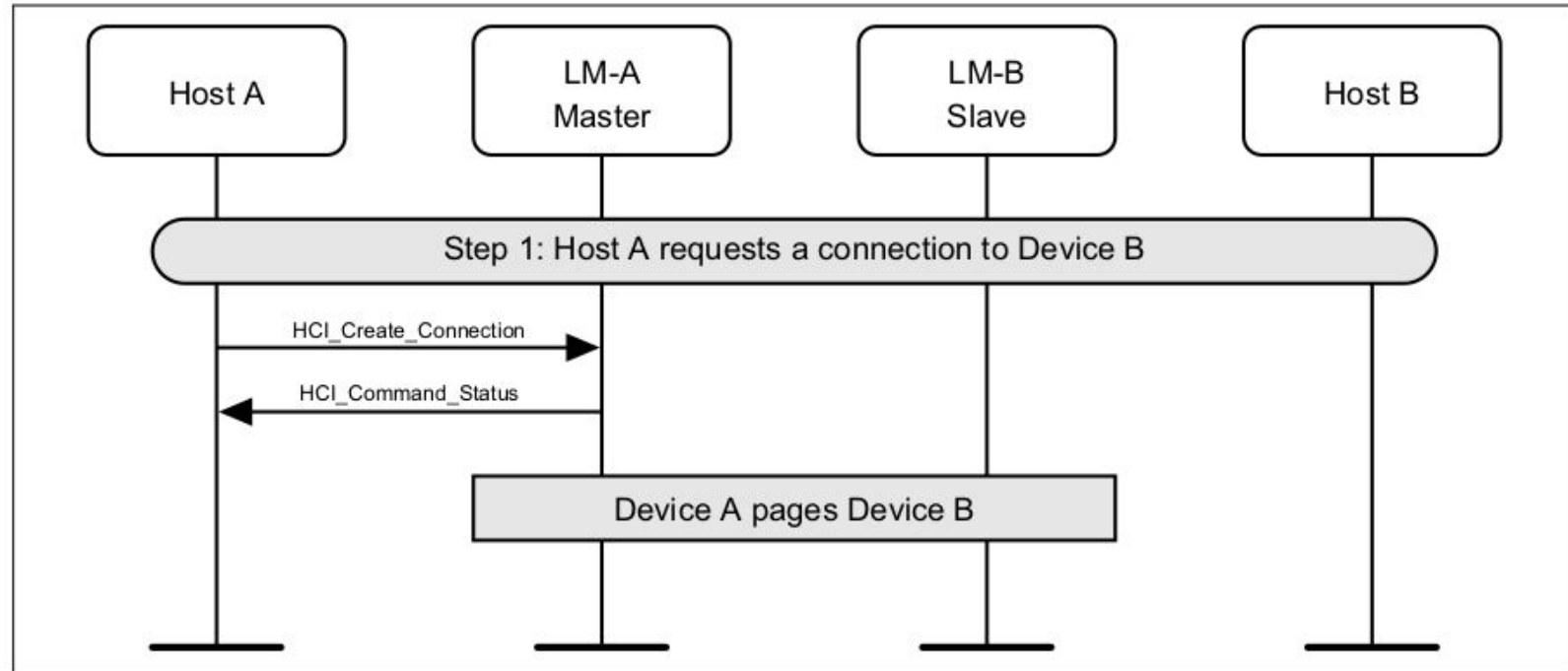
Descubrimiento de dispositivos

Bluetooth LE Escaneo activo



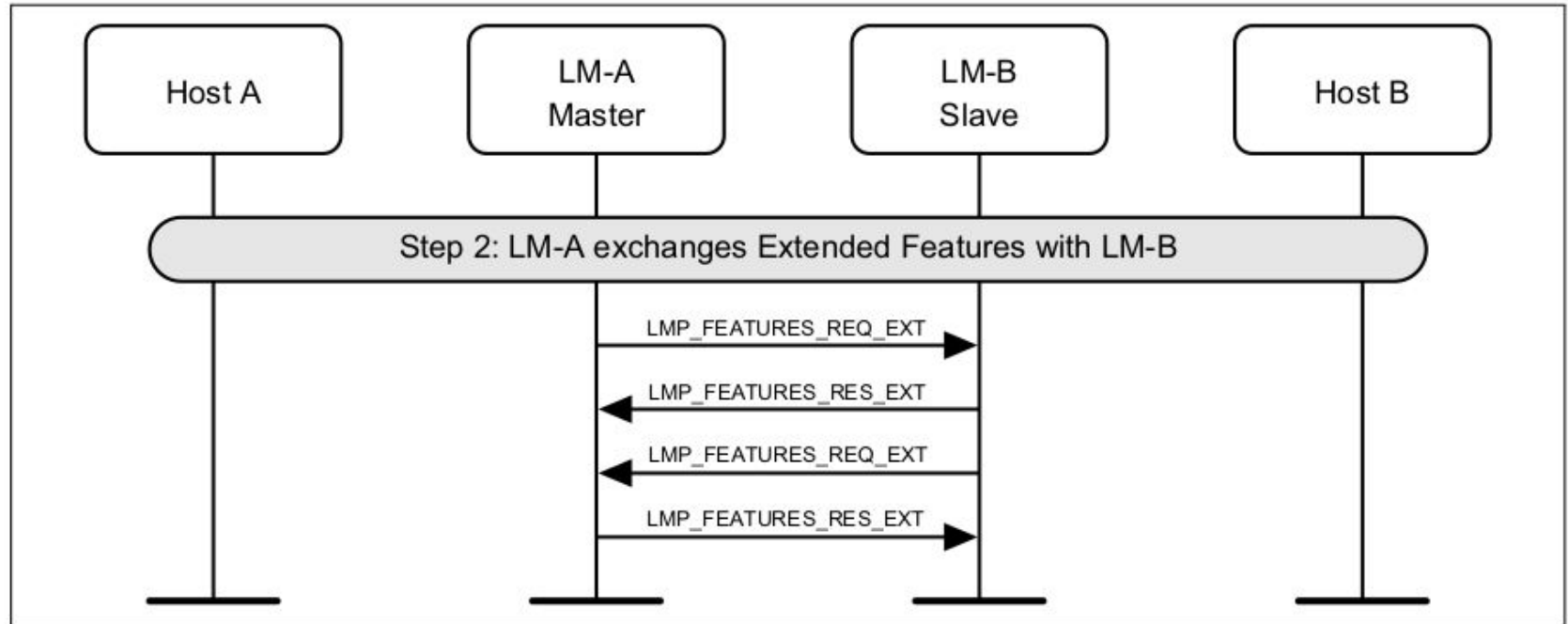
Establecimiento y liberación de conexión entre dispositivos

Bluetooth BR/EDR Establecimiento de conexión

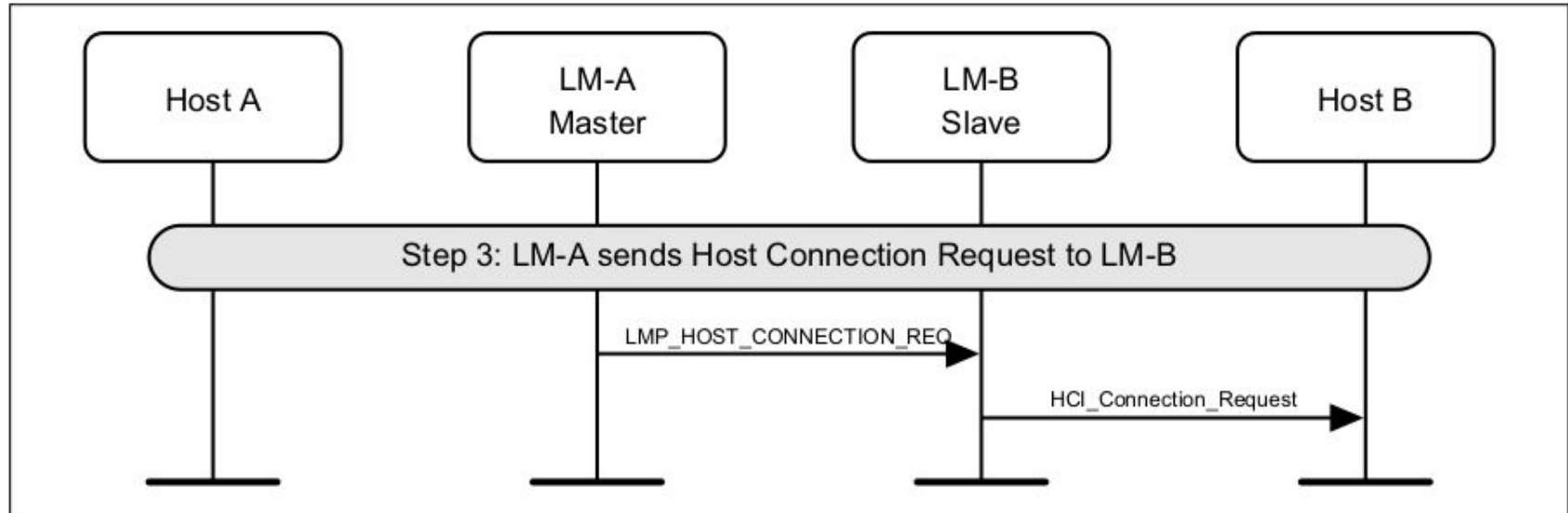


Establecimiento y liberación de conexión entre dispositivos

Bluetooth BR/EDR Establecimiento de conexión

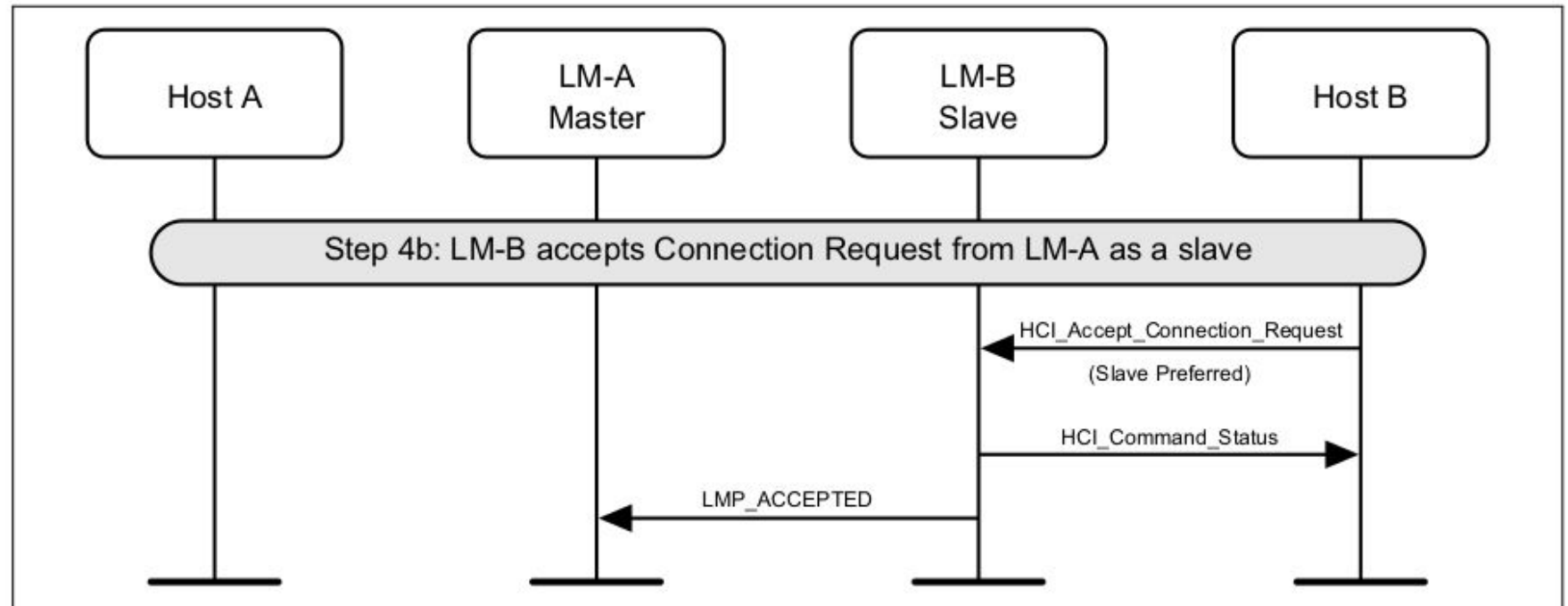


Bluetooth BR/EDR Establecimiento de conexión



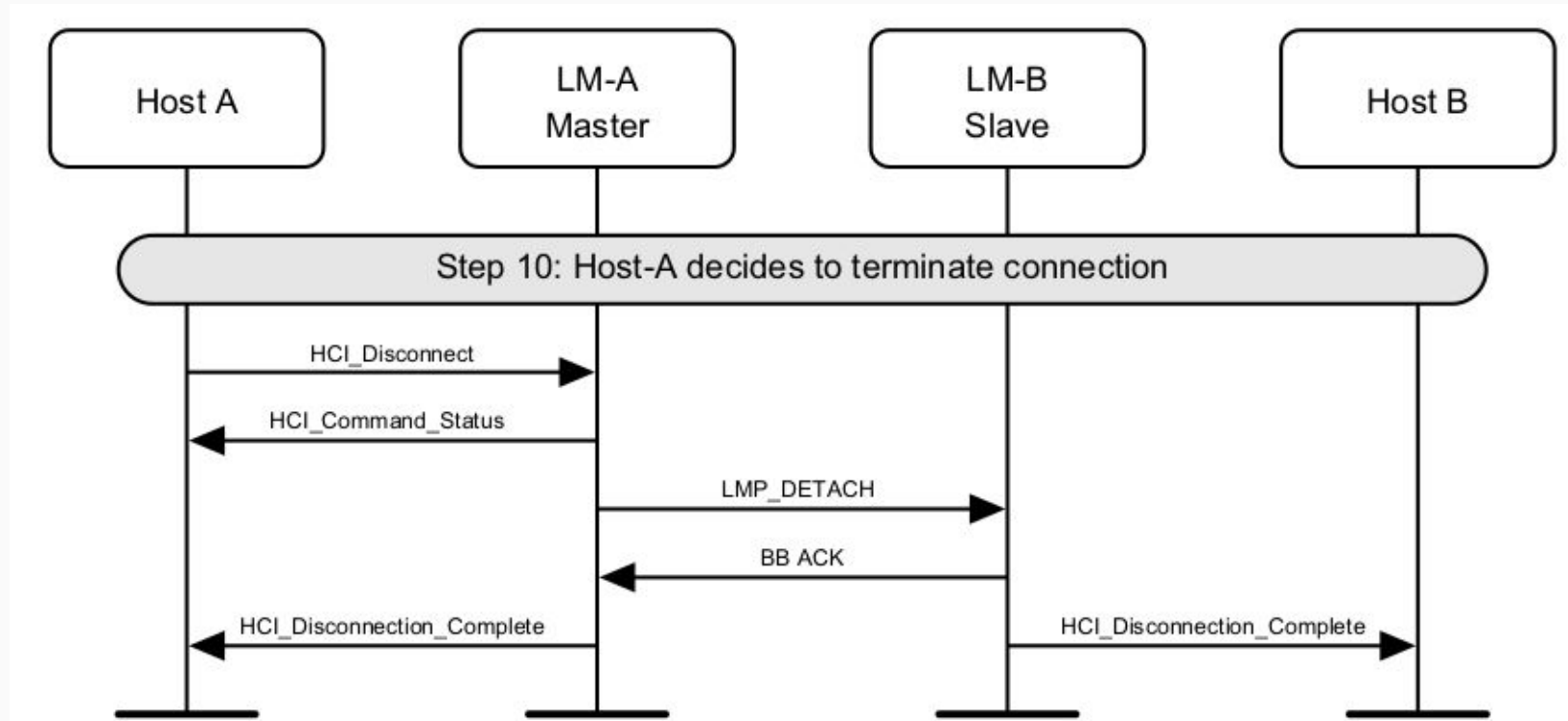
Establecimiento y liberación de conexión entre dispositivos

Bluetooth BR/EDR Establecimiento de conexión



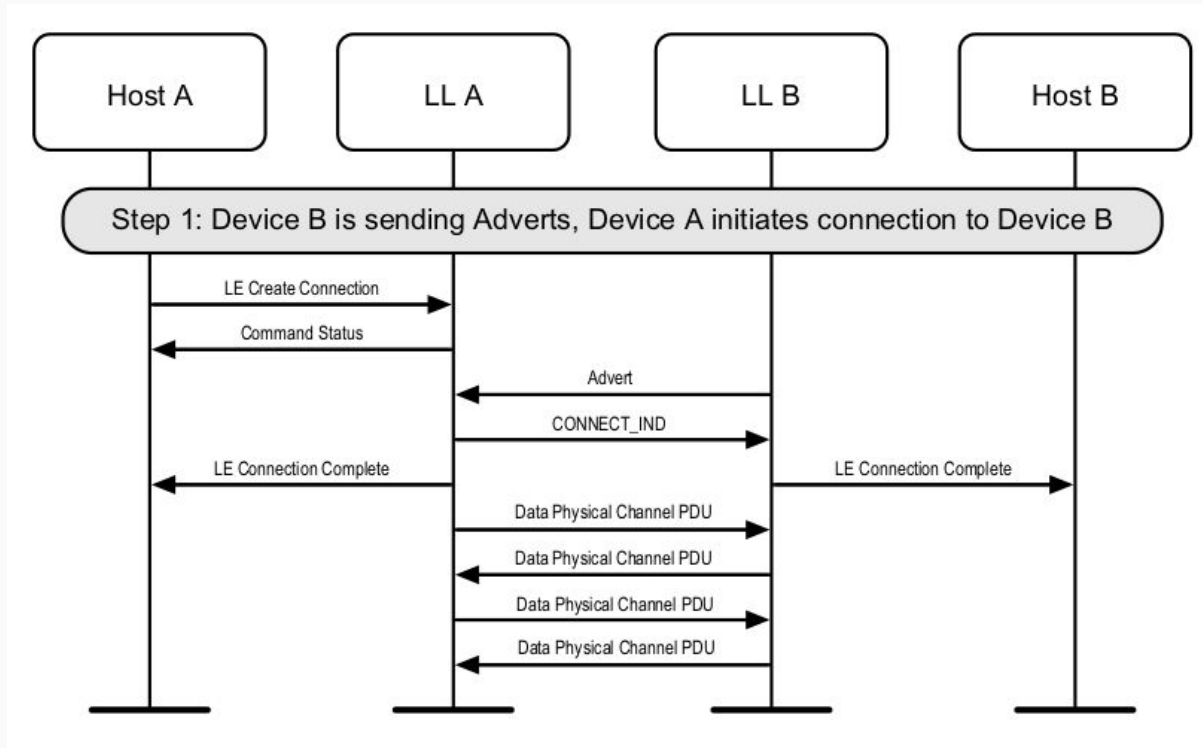
Establecimiento y liberación de conexión entre dispositivos

Bluetooth BR/EDR Liberación de conexión



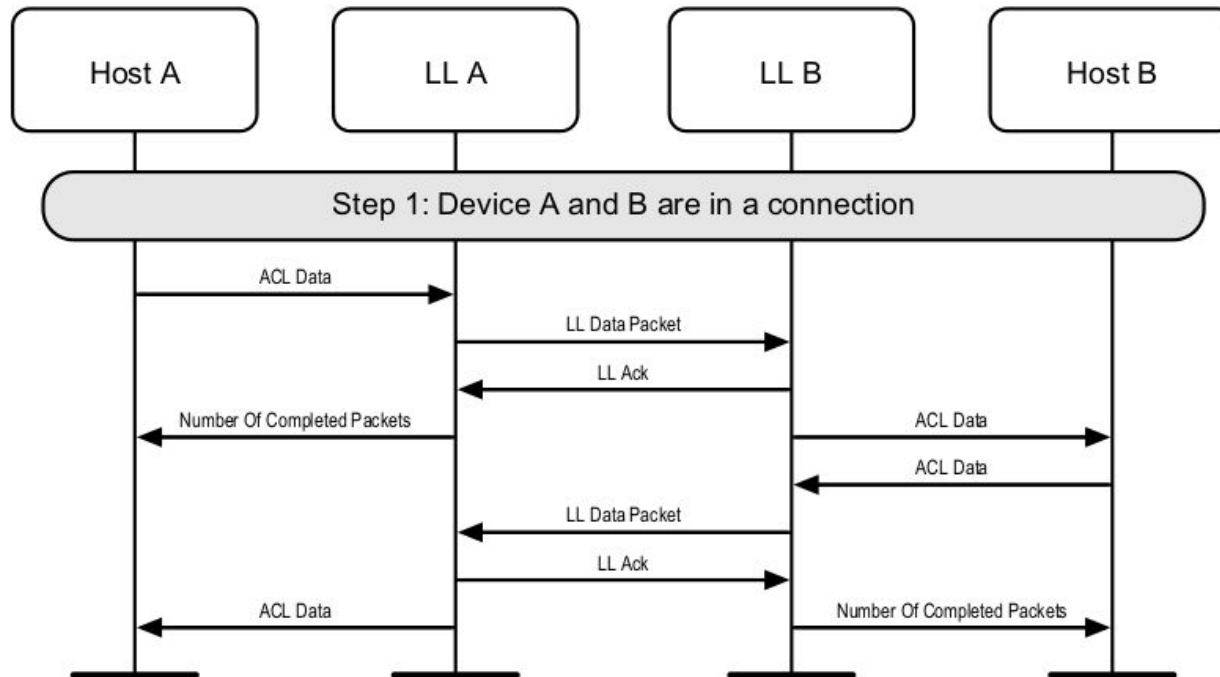
Establecimiento y liberación de conexión entre dispositivos

Bluetooth LE Establecimiento de conexión



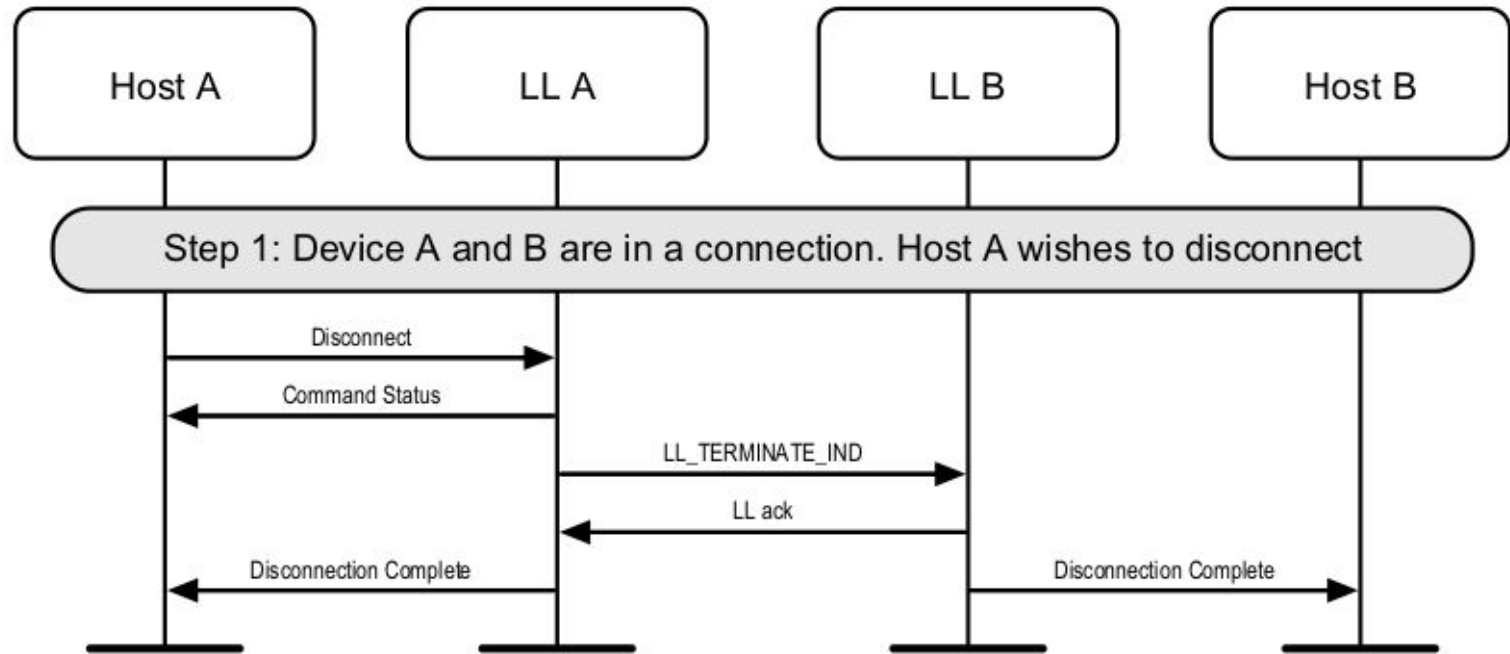
Establecimiento y liberación de conexión entre dispositivos

Bluetooth LE Envío de datos



Establecimiento y liberación de conexión entre dispositivos

Bluetooth LE Liberación de conexión



Bibliografía

- [Core Specifications | Bluetooth® Technology Website](https://www.bluetooth.com/specifications/bluetooth-core-specification/)
(<https://www.bluetooth.com/specifications/bluetooth-core-specification/>)