Redes Inalámbricas

Bluetooth

Pablo Serrano

Grados de informática

Universidad de Málaga

Introducción

- Los estándares que se ocupan de la especificación de la transmisión inalámbrica y la técnica de control de acceso al medio en redes de área personal y local inalámbricas son el IEEE 802.11 y IEEE 802.15
- IEEE 802.15 es un grupo de trabajo dentro de IEEE 802 especializado en redes inalámbricas de área personal (wireless personal area networks, WPAN) (redes tipo PAN o HAN, centradas en las cortas distancias)
- Al igual que Bluetooth o ZigBee, el grupo de estándares 802.15 permite que dispositivos portátiles como PC, teléfonos, sensores y actuadores utilizados en domótica, entre otros, puedan comunicarse e interoperar

Wireless Personal Area Network

- Una red inalámbrica de área personal (WPAN) es una red de área personal en la que las conexiones son inalámbricas
  - Basadas en el estándar IEEE 802.15
- Tecnologías utilizadas:
  - Infrarrojos
  - Radiofrecuencia
- La conexión se realiza por proximidad
- Cada dispositivo puede bloquear la conexión con otros dispositivos, impidiendo interferencias o acceso no autorizado a la información

Bluetooth

- Fue desarrollado inicialmente como un proyecto de la compañía Ericsson
- Debe su nombre a Harald Blaatand, el rey de Dinamarca (940-981) que unió Dinamarca y Noruega
- El logo de Bluetooth son las runas de las iniciales del nombre y el apellido
  - ᚼ (Hagall)
  - ᛒ (Berkana)
- Hoy día sigue el estándar IEEE 802.15.1

Usos

- Nace con el objetivo de realizar comunicaciones de corto alcance como IrDA, pero sin la limitación de la visibilidad
- Es posible crear pequeñas redes con:
  - Reproductores de música
  - Localizadores GPS
  - Periféricos (teclados, ratones, impresoras, etc.)
- BLE (Bluetooth Low Energy)
  - Telemedicina (termómetros, tensiómetros, glucómetros, etc.)
  - Rastreo

Versiones

- v1.0 y v1.0b (1999)
  - v1.1 (2002) – Corrige muchos errores en las especificaciones
  - v1.2 (2003) – 720 Kbps
- v2.0 (2004) – 3 Mbps (EDR: enhanced data rate)
  - v2.1 (2007) – Mejoras en el emparejamiento (SSP: Secure Simple Pairing)
- v3.0 (2009) – 24 Mbps (especificación High Speed)
- v4.0 (2010) – Incorporación de especificación BLE (antes WiBree), cobertura y tasa de transferencia mejoradas (32 Mbps)
- v5.0 (2016) – 50 Mbps (influye la cercanía), multiplica el alcance por 4
  - v5.1 (2019) – Detección de ubicación de otros dispositivos
  - v5.2 (2020) – Mejoras BLE
  - v5.3 (2022) – Mejoras en eficiencia y consumo
  - v5.4 (2023) – Comunicación bidireccional entre AP y nodos de baja potencia

Características

- Banda ISM (2.45 GHz)
- Al ser una banda abierta, se debe usar un mecanismo para proteger de interferencias
- Espectro ensanchado con saltos de frecuencia (frecuency hopping)
  - División de la banda de trabajo en varios canales
  - Cambio constante de canales durante la conexión de forma pseudoaleatoria
  - Ancho de banda instantáneo pequeño
  - Propagación eficiente sobre el ancho de banda total
- Se consigue tener transceptores de banda estrecha con una gran inmunidad frente a interferencias

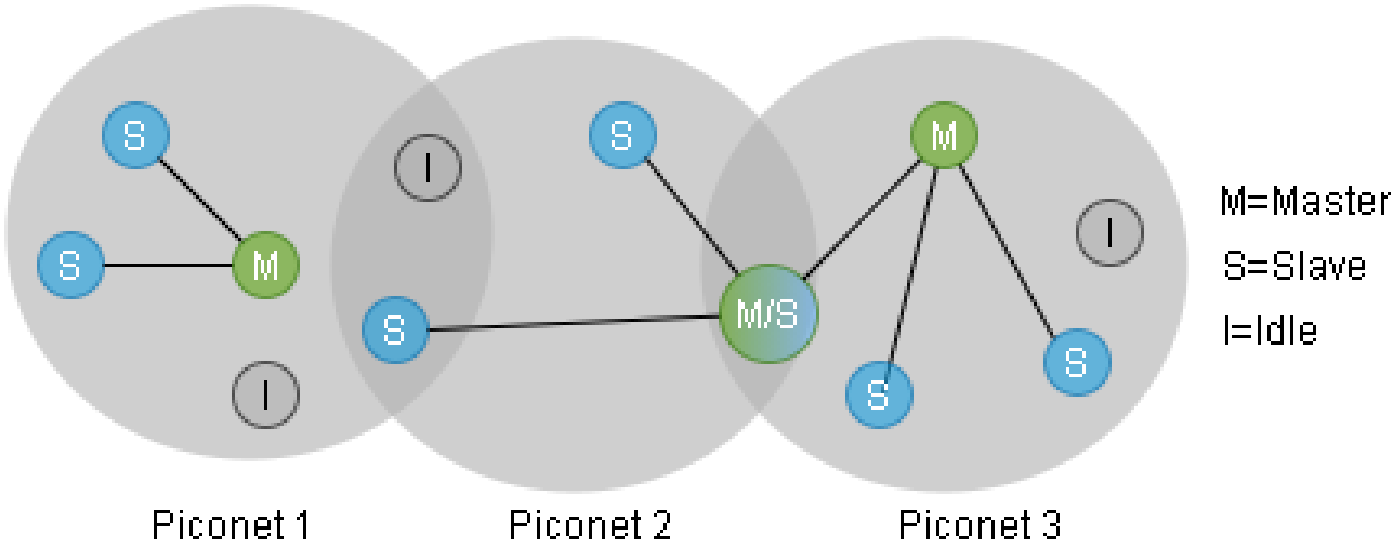
Topología

- Picorred (piconet)
  - Red de corto alcance formada por dos o más dispositivos (hasta 8 activos)
  - Canal síncrono
  - Saltos de frecuencia propios, distintos de las piconets adyacentes
  - Dispositivo maestro (Master) o primario (único por picorred)
    - Responsable de la sincronización
    - Determina los saltos de frecuencia
    - Busca dispositivos
    - Establece conexiones
  - Dispositivos esclavos (Slaves) o secundarios
    - Se sincronizan con el maestro una vez conectados

Topología

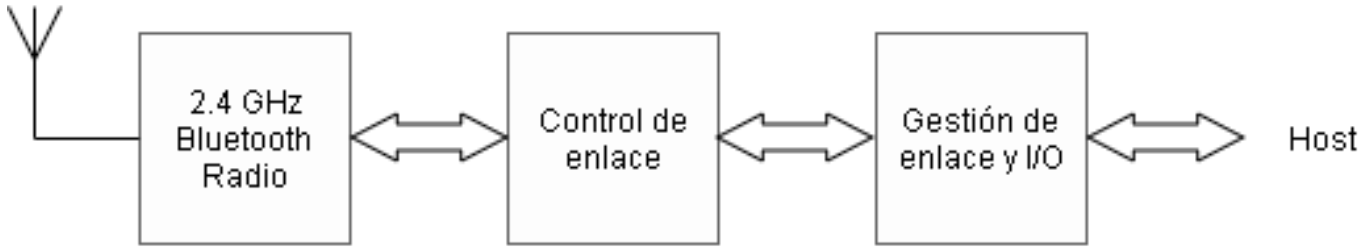
- Máximo 7 canales de datos por piconet, de hasta 721 Kbps en la especificación básica
  - 8 dispositivos por piconet
  - Puede haber más esclavos en estado aparcado (parked) (hasta 255)
    - Están inactivos pero sincronizados con el maestro
- Scatternet (red dispersa)
  - Red ad-hoc de varias piconets (hasta 10)
  - Una misma estación puede ser miembro de dos picorredes:
    - Como esclavo de dos piconets
    - Como maestro en una y esclavo en otra. Este dispositivo puede recibir mensajes del maestro en la primera picorred (como esclavo) y actuando como maestro, entregarlos en la segunda picorred.
  - No existe sincronización entre piconets
  - Un dispositivo que pertenezca a varias solo podrá estar activo en una al mismo tiempo

Topología

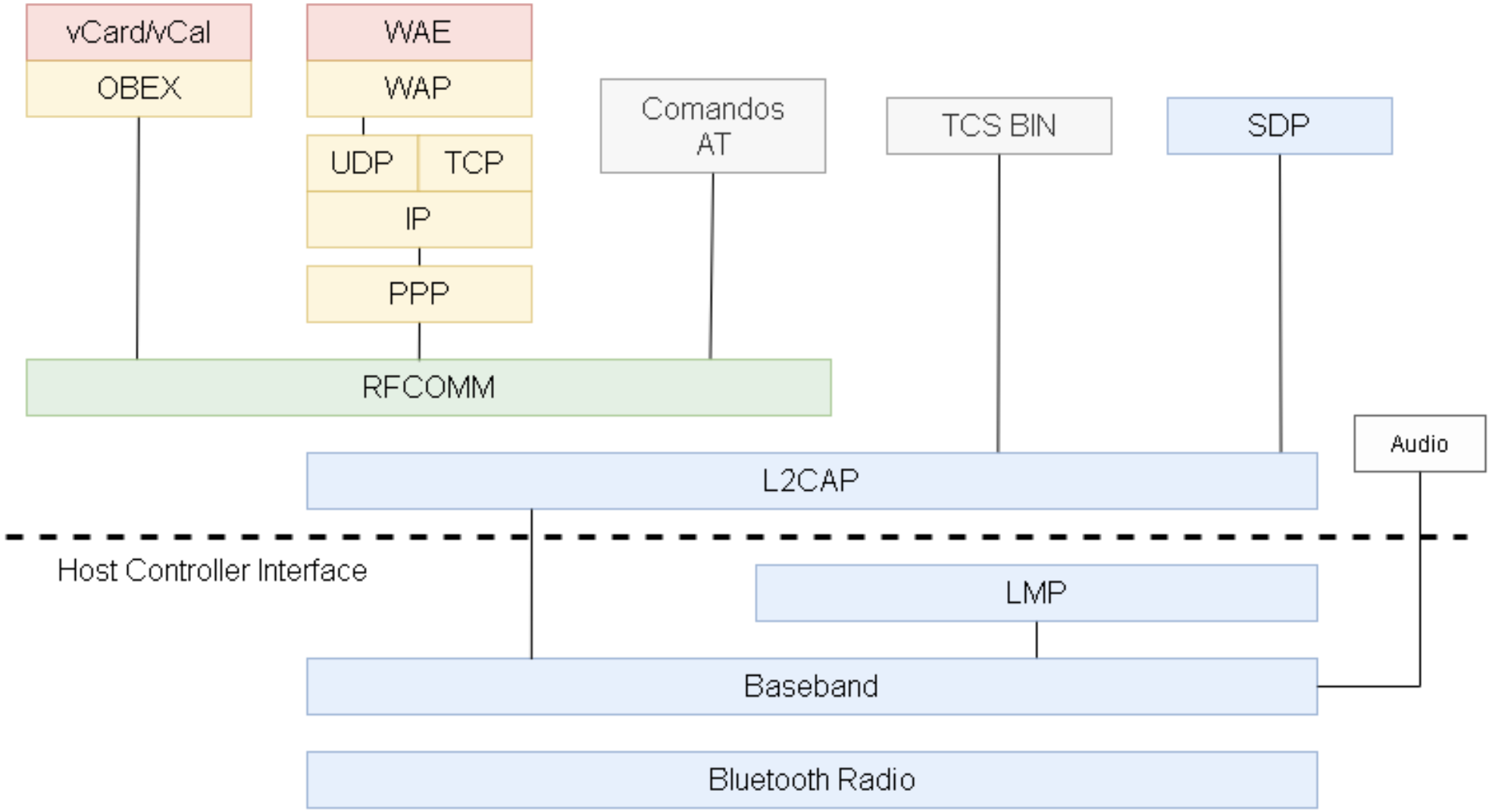

S
S
M
I
I
S
M/S
S
M
I
S
S
M=Master
S=Slave
I=Idle
Piconet 1
Piconet 2
Piconet 3

Bloques funcionales

- Transceptor RF + antena
- Unidad de control de enlace en banda base
- Software de gestión en el host



Pila de protocolos



Pila de protocolos

- Protocolos propios y otros ya existentes
- Propios
  - LMP (Link Manager Protocol)
  - L2CAP (Logical Link Control and Adaptation Protocol)
- Otros
  - Bluetooth SIG
  - OBEX (Object Exchange Protocol)
  - PPP (Point to Point Protocol)

Core o especificación principal

- Protocolo de nivel físico (PHY) y acceso al medio (MAC)
  - 4 protocolos inferiores
  - Descubrimiento de servicios (SDP: Service Discovery Protocol)
  - Perfil de acceso genérico GAP
- Controlador Bluetooth
  - Radiofrecuencia
  - Banda base
  - Gestión de enlace (LMP: Link Manager Protocol)
- Resto de niveles por encima del HCI (Host Controller Interface)
  - Software en el host Bluetooth
  - Comunicación con el controlador utilizando un interfaz estándar
  - Nivel más importante: Control y adaptación del enlace lógico (L2CAP)

Nivel de radiofrecuencia

- Equivalente al nivel físico OSI
- Los dispositivos Bluetooth son de baja potencia y tienen un rango desde 10 a 100 metros
- Utiliza la banda ISM (industrial, scientific and medical) de 2,4 GHz dividida en 79 canales de 1 MHz cada uno
- Utiliza el método de espectro ensanchado por salto de frecuencias (FHSS) para evitar las interferencias de otros dispositivos y redes

Frequency Hopping Spread Spectrum

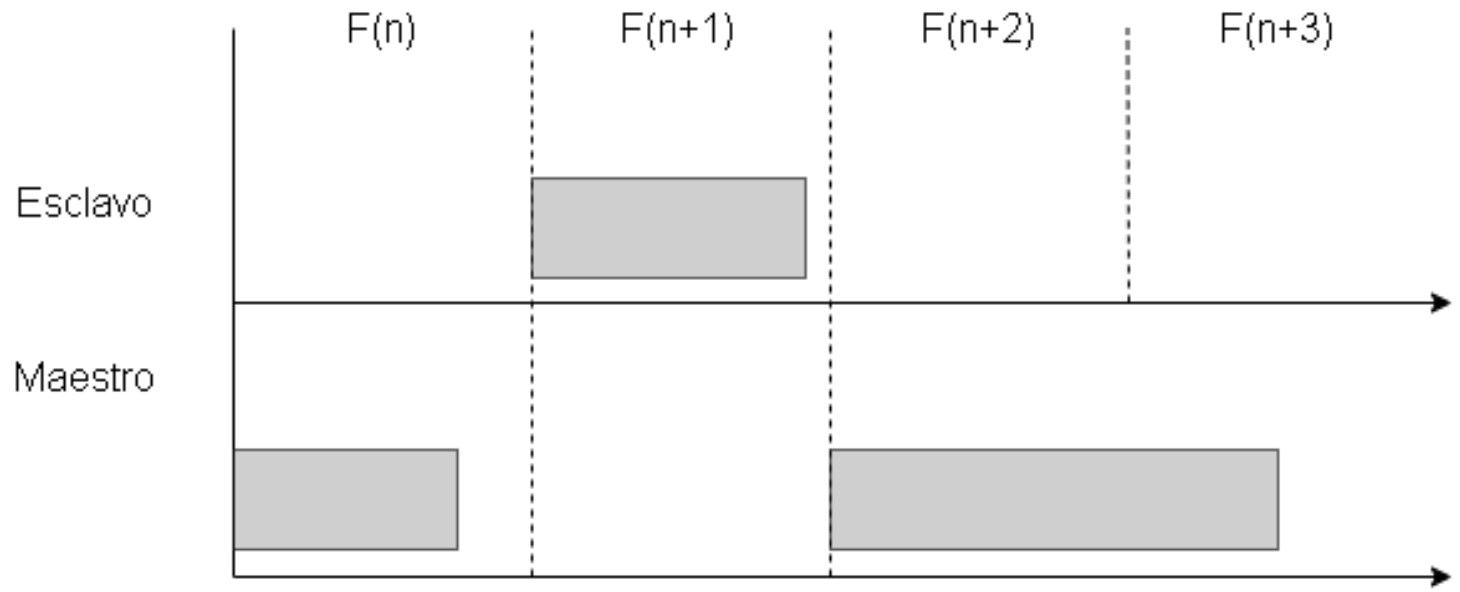
- Inventado por Hedy Lamarr y George Antheil en 1941
- Su invención era un prototipo de lo que luego se conoció como “técnica de salto en frecuencia”, y sirvió para construir torpedos teledirigidos por radio que no pudieran ser detectados por los enemigos
- Patentó un sistema electrónico de comunicaciones entre aviones y barcos para dirigir un torpedo con señales de radio cortísimas que cambian de frecuencia arbitraria y simultáneamente para evitar ser interceptadas
- Una frecuencia en constante cambio no puede ser bloqueada
- Es el germen de sistemas como el GPS, Bluetooth, teléfono móvil y wifi. También trabajó en un escudo antiaéreo
- Antheil le dio a Lamarr la mayor parte del crédito, aunque él proporcionó una parte importante: “la técnica del pianista”
  - Usó un teclado de piano modificado en el torpedo y el transmisor, de forma que las frecuencias cambiantes (88) siempre estarían en sincronía

Nivel de banda base

- Equivalente al subnivel MAC
  - Establecimiento de conexión, direccionamiento, formateo paquete, sincronización y control de potencia
- El método de acceso es una forma de TDMA (Acceso Múltiple por División en el Tiempo)
  - Las estaciones comparten en el tiempo el ancho de banda del canal
  - Cada estación tiene asignada una ranura de tiempo (slot) durante el cual puede enviar datos
  - Las estaciones tienen que estar sincronizadas (conocer el comienzo y posición de su ranura)
- La comunicación ocurre solo entre el maestro y el esclavo. Los esclavos no pueden comunicarse directamente entre sí
- Controla los saltos de frecuencia
  - 16000 / s -> la longitud de una ranura es 625 microsegundos (tiempo *dwell*)

Nivel de banda base

- Todos los dispositivos están sincronizados con el canal en salto y tiempo
- En una transmisión cada paquete debe estar alineado con el inicio de un slot y puede tener una duración de 1, 3 o 5 slots
- Para evitar fallos en la transmisión, el maestro envía en los slots pares y los esclavos en los impares.



Nivel de banda base: modos de funcionamiento

- No orientado a conexión asíncrono (ACL, Asynchronous Connection-Less)
  - Conmutación de paquetes con confirmación: se usa cuando la integridad (entrega libre de errores) es más importante que la latencia (retardo en la entrega de datos)
  - Para paquetes de datos generales
  - Conexiones simétricas o asimétricas y punto a multipunto
  - Acceso al medio mediante multiplexación en el tiempo
  - Un esclavo devuelve una trama ACL en la ranura impar disponible si y solo si el paquete de la ranura anterior era para él
  - Se consigue una tasa máxima de transferencia más alta que con SCO
  - El BW del enlace debe ser configurado y aceptado por los dos dispositivos antes de la transmisión de paquetes
  - Retransmisión si no son confirmados: protección frente a interferencias
  - Desconexión automática del enlace después de un tiempo sin transmitir (unos 20s)

Nivel de banda base: modos de funcionamiento

- Síncrono (SCO, Synchronous Connection-Oriented)
  - Si se daña un paquete no es retransmitido: se usa cuando es más importante la latencia que la integridad
  - Para datos de voz en tiempo real
  - Punto a punto
  - Ancho de banda fijo
  - Slots temporales reservados dentro de un enlace ACL (dos, uno por sentido)
  - Cada dispositivo transmite datos de voz en uno de los slots reservados

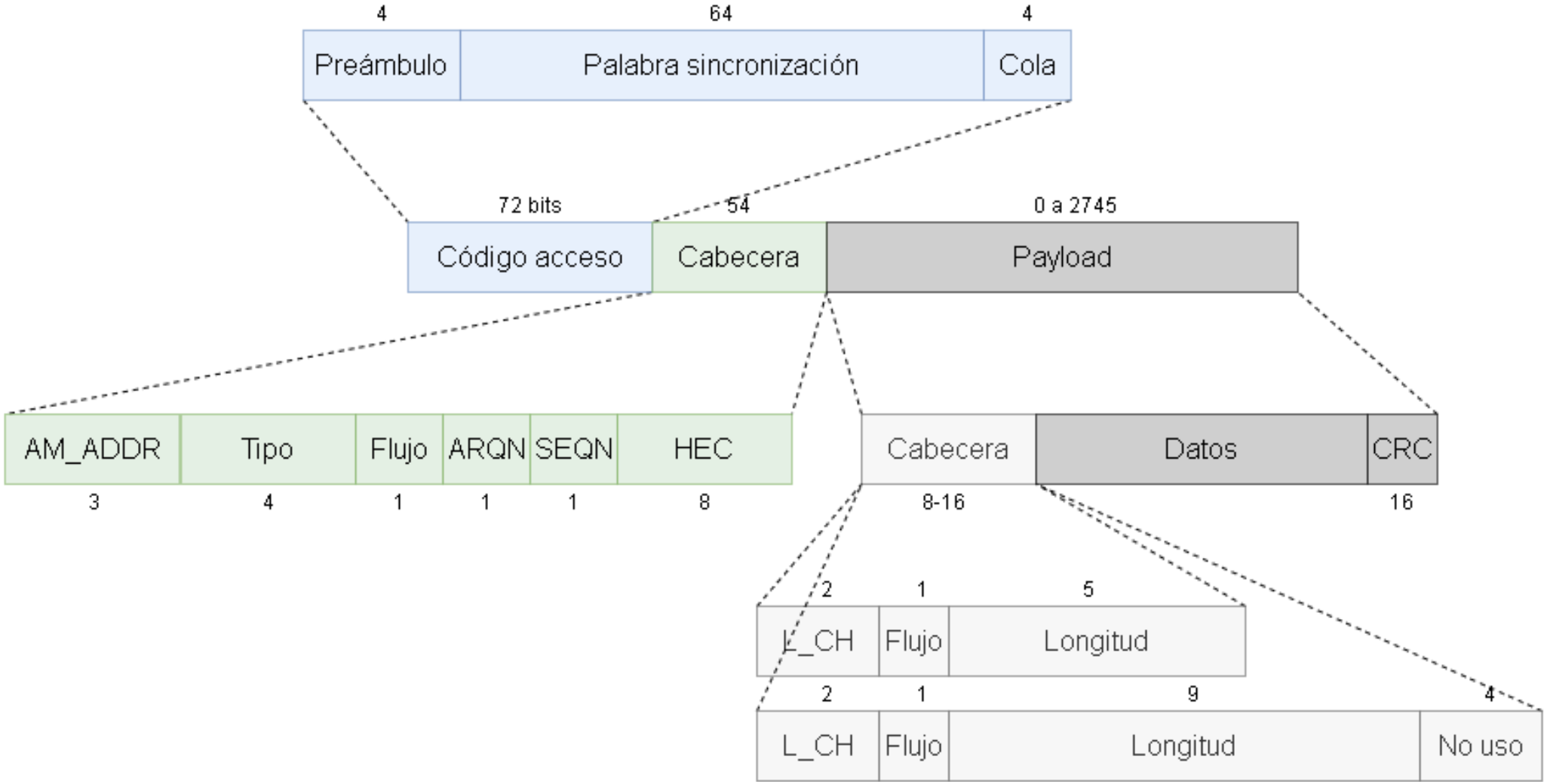
Transmisión de paquetes en una piconet

- El paquete general está formado por tres campos:
  - Código de acceso
    - Sincronización e identificación para el paquete
    - Tres tipos:
      - De acceso al canal (identifica una piconet)
      - De acceso al dispositivo (para procedimientos de señalización especiales)
      - De acceso de búsqueda (IAC, Inquiry Access Code)
        - Descubrir a otros dispositivos Bluetooth dentro del rango
    - Formado por un preámbulo, una palabra de sincronización y una cola

Transmisión de paquetes en una piconet

- Cabecera (flags)
  - Dirección del dispositivo dentro de la piconet (3 bits)
  - Tipo de paquete
  - Control de flujo: indica que el buffer de recepción se ha llenado
  - Confirmación de recepción (ARQN: Automatic Retransmission Query Numbering)
  - Bit de secuencia (SEQN, Sequential Numbering): indica si el paquete es el esperado o se trata de una retransmisión
  - Chequeo de redundancia cíclica de cabecera para el control de errores (HEC, Header Error Control/Check)
- Payload (información a transmitir)
  - Cabecera
  - Datos
  - CRC

Formato de los paquetes



Descubrimiento de dispositivos

- La única forma de que un dispositivo detecte a otro es iniciar el proceso de descubrimiento de dispositivos
- Detectabilidad vs conectividad
  - Por cuestiones de ahorro de energía y privacidad, todos los dispositivos Bluetooth admiten dos configuraciones que determinan si el dispositivo responderá o no a la peticiones de detección (descubrimiento) y de conexión.
- Inquiry Scan
  - Controla las peticiones de descubrimiento
  - ON es descubrible
- Page Scan
  - Controla las peticiones de conexión
  - ON acepta peticiones de conexión entrantes

Detectabilidad vs conectividad

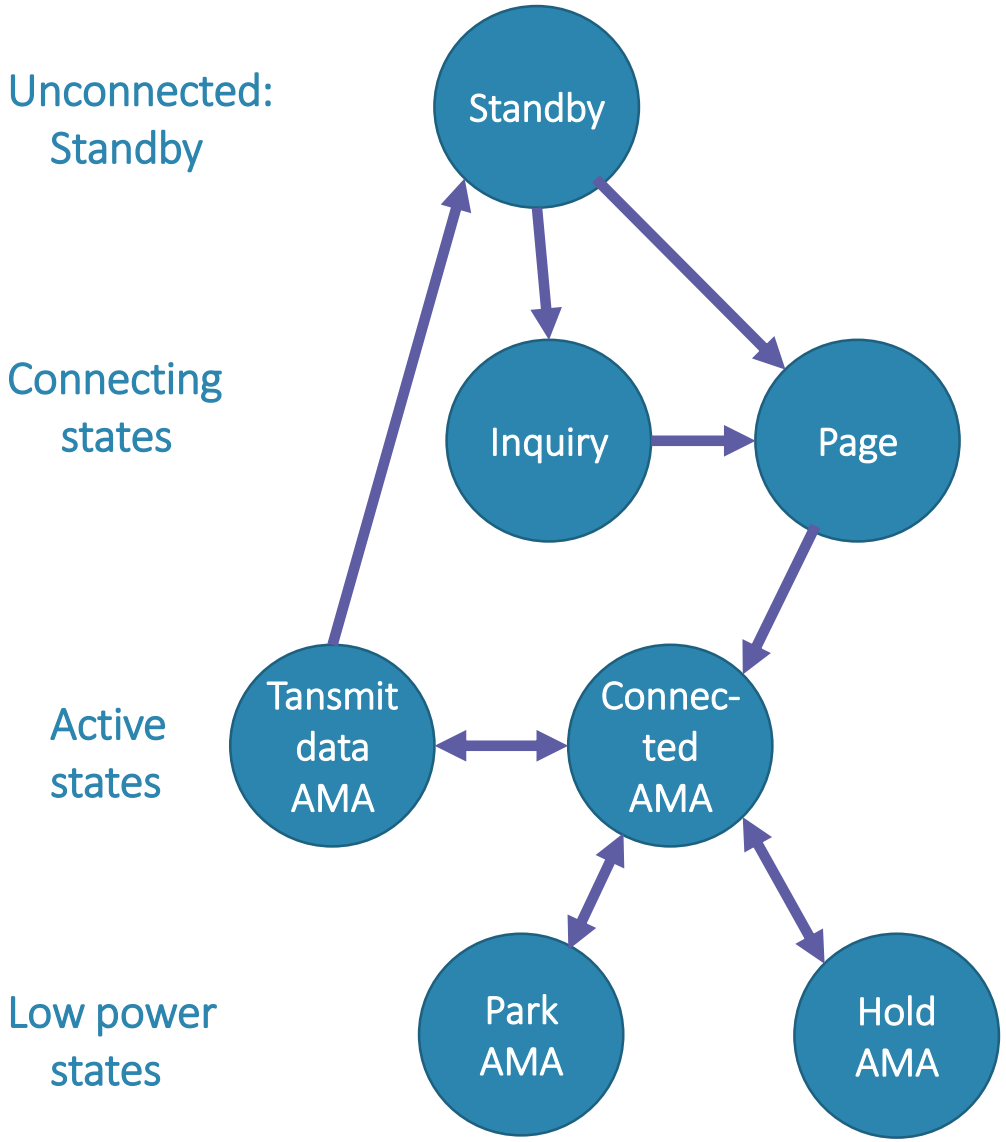
Inquiry Scan	Page Scan	Interpretación
ON	ON	Es detectable y acepta peticiones de conexión entrantes (Defecto)
OFF	ON	No es detectable y acepta peticiones de conexión entrantes realizadas por dispositivos que tenían previamente su dirección (Defecto)
ON	OFF	Es detectable pero no acepta peticiones de conexión entrantes
OFF	OFF	No es detectable y no acepta peticiones de conexión entrantes. El dispositivo sólo establece conexiones de salida.

Descubrimiento de dispositivos: procedimiento

- Pregunta o Inquiry: permite al maestro descubrir los dispositivos disponibles para unirse a la red
- Emite mensajes de forma continuada (no especifica la fuente, pero puede especificar el tipo de dispositivo que busca). Para garantizar que un dispositivo que está buscando otros dispositivos pueda localizar todos los dispositivos en modo inquiry scan que están en rango, la especificación Bluetooth define un tiempo de búsqueda de 10,24 segundos
- Los dispositivos disponibles contestan incluyendo sus propios parámetros y entran en modo Inquiry Scan
- El maestro puede establecer conexión con uno de estos dispositivos usando los parámetros recibidos
- Transmite el código de acceso del dispositivo esclavo (DAC, Device Access Code): estado de Paging o Búsqueda
- El esclavo que recibe su propio DAC responde
- El maestro envía la información de sincronización (FHS, Frequency Hop Synchronization)
- El esclavo establece la conexión y se sincroniza con la piconet, actualizando su código de acceso al canal y su reloj con la información de la red y de la secuencia de saltos recibida en el FHS

Diagrama de estados del protocolo banda base

- Standby
  - Esperando a unirse a una piconet
- Inquire
  - Buscando dispositivos disponibles
- Page
  - Conectado a un dispositivo
- Connected
  - Activo en una piconet (maestro o esclavo)
- Park/Hold
  - Estados de baja potencia



Releases AMA (active member address)

Limitaciones de Bluetooth

- No es posible:
  - Anunciar la presencia de un dispositivo
    - Excepto BLE advertising
  - Detectar cuándo un dispositivo remoto está preguntando (inquiry) por dispositivos cercanos
  - Determinar la dirección Bluetooth del dispositivo que pregunta
  - Saber la distancia entre dos dispositivos
    - Hasta v5.1
  - Difundir mensajes (broadcast) (a pesar de que L2CAP lo permite)
    - Para establecer una comunicación, los dispositivos necesitan estar emparejados
    - Solo de tipo advertising, en BLE

Nivel de gestión de enlace (LMP, link management protocol)

- Control del enlace radio entre dos dispositivos, controlando el canal físico (banda base) para el establecimiento del enlace radio y su finalización
  - Realizado por el Link Manager
- También labores de control de tráfico y de consumo
- Permite intercambiar mensajes entre dos dispositivos Bluetooth en su radio de acción, para el establecimiento de un enlace
- Realiza autenticación y cifrado
- Especifica PDUs (Protocol Data Units) obligatorias y otras opcionales, aunque recomendadas
- Tras el paging:
  - Solicitar identidad y autenticar dispositivos
  - Establecer el tipo de enlace (ACL o SCO)
  - Determinar el tipo de trama a usar
- Los mensajes de esta capa no viajan hacia niveles superiores y tienen un nivel de prioridad mayor

L2CAP

- Control y adaptación de enlace lógico (Logical Link Control and Adaptation Protocol)
- Adaptar el funcionamiento de los protocolos de capas superiores, como SDP (Service Discovery Protocol) o RFCOMM (Radio Frequency Communication), al nivel de banda base, multiplexando los datos
- Segmentación y reensamblado
- Gestión de QoS (Quality of Service)
- Canal L2CAP
  - Representa un flujo de datos (paquetes) entre dos entidades
  - Orientados o no a conexión
- Fragmentación en varios paquetes de nivel banda base

Protocolo de descubrimiento de servicios (SDP)

- Proporciona a las distintas aplicaciones cliente la posibilidad de descubrir qué servicios están disponibles en el servidor y sus características
- Los registros de servicio contienen la descripción de servicios determinados
- Cada propiedad de un registro, consta de:
  - Identificador de propiedad: único de 16 bits
  - Valor de longitud variable y contiene la información sobre el servicio
- Pasos:
  - Petición de búsqueda de servicio(s) por parte del cliente
    - Algunos (con un patrón de búsqueda)
    - Todos (browsing)
  - El servidor busca en sus registros y responde
  - El cliente puede solicitar más información sobre alguno incluyendo propiedades deseadas
  - El servidor responde

Protocolo de comunicación de RF (RFCOMM)

- Emulación de puertos serie sobre el protocolo L2CAP
- Emulación de interfaz serie RS-232
- Soporta emulación de 60 conexiones simultáneas que son multiplexadas
- Basado en el estándar TS 07.10 del ETSI
- Orientado a hacer más flexibles los dispositivos que requieren el uso de puertos serie
- Ej.: PPP, Point to Point Protocol

Perfiles Bluetooth (Bluetooth Profiles)

- Son un conjunto de mensajes y procedimientos para escenarios y modelos de uso concretos del dispositivo
- Definen formas estándar para servicios Bluetooth que un dispositivo puede ofrecer o utilizar
  - Intercambio de archivos, sonido estéreo, compartir datos, usar impresoras…
- Ventajas:
  - Permiten que no sea necesario implementar en un dispositivo toda la pila de protocolos, sólo los necesarios
  - Aseguran la interoperabilidad entre varias unidades Bluetooth que cumplan los mismos perfiles, aunque sean de distintos fabricantes
- Es necesario implementar al menos un perfil
- Incluyen
  - Información sobre dependencia de otros perfiles
  - Propuestas de interfaz de usuario
  - Características concretas de la pila e protocolos Bluetooth que utiliza

Perfiles básicos Bluetooth

- GAP (Generic Access Profile)
  - Sirve de base para el desarrollo de otros perfiles
  - Establece procedimiento para crear enlaces de banda base entre dispositivos
  - Información sobre las funciones que debe implementar todo dispositivo Bluetooth
  - Procedimientos generales para la detección de dispositivos (Discovery)
  - Procedimientos generales para la conexión
  - Formato básico de interfaz de usuario

Perfiles básicos Bluetooth

- Perfil de Aplicación del descubrimiento de Servicio (SDAP)
  - Define los procedimientos para descubrir servicios registrados en otros dispositivos
- Perfil de Puerto Serie (SPP)
  - Define los procedimientos para poder simular el puerto serie en los dispositivos Bluetooth. Permite conexiones RFCOMM entre dos dispositivos Bluetooth como si se tratara de una conexión serial cableada(RS-232)
- Perfil genérico de intercambio de objetos (GOEPOBEX)
  - Este perfil define cómo los dispositivos Bluetooth deben soportar los modelos de intercambio de objetos

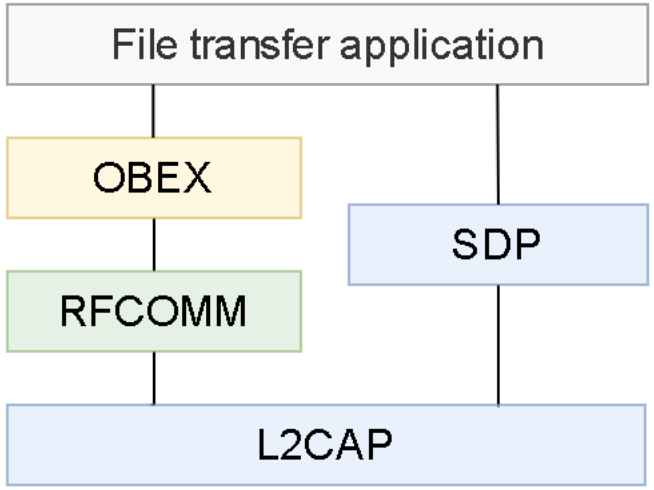
Perfiles Bluetooth

- DUN (Dial-Up Networking)
  - Acceso telefónico estándar a Internet
  - Ej.: acceso a Internet desde un portátil usando el teléfono móvil como módem, que realiza el marcado de forma inalámbrica
- File transfer
  - Permite a un dispositivo acceder al sistema de ficheros de otro dispositivo y enviar o recibir ficheros, copiar, renombrar, …
- HFP (Hands Free Profile) (perfil manos libres)
  - Configura un teléfono móvil como puerta de enlace
  - Realizar y recibir llamadas usando un dispositivo manos libres
- HID (Human Interface Device) (perfil de dispositivo de interfaz humana)
  - Interfaces de usuario como teclados, ratones o punteros, o dispositivos de control remoto

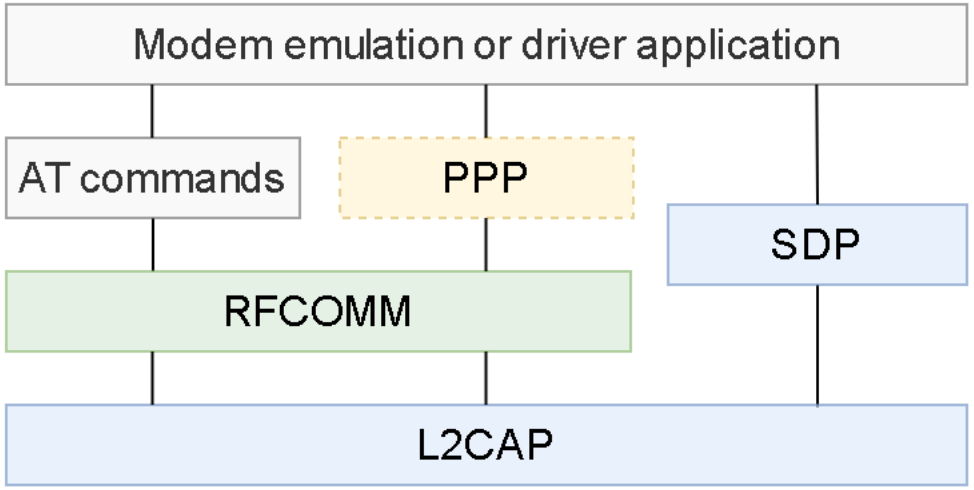
Perfiles Bluetooth

- A2DP (Advanced Audio Distribution Profile) (Perfil de distribución de audio)
  - Transferencia de sonido estéreo de alta calidad de una fuente de sonido a un dispositivo receptor
  - Calidad de audio superior a la tradicional distribución de señales de audio que puede realizar Bluetooth a través de los canales SCO (Synchronous Connection-Oriented)
- HCRP (Hardcopy Cable Replacement Profile)
  - Impresión de archivos
  - Funcionamiento cliente/servidor: ordenador/impresora
- HSP (HeadSet Profile)
  - Auriculares
- PAN (Personal Area Networking)
  - Permite formar redes IP y, especialmente, compartir la conexión a Internet de un dispositivo con otro (Tethering)

Perfiles Bluetooth: modelos de uso

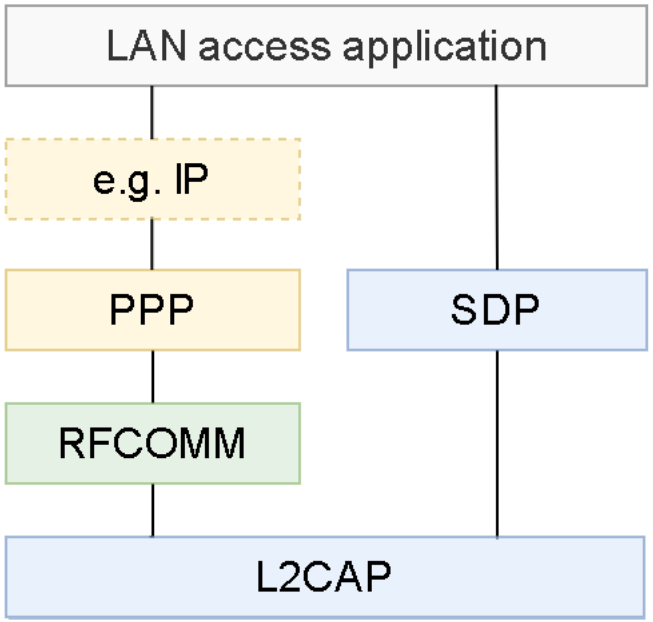


File transfer

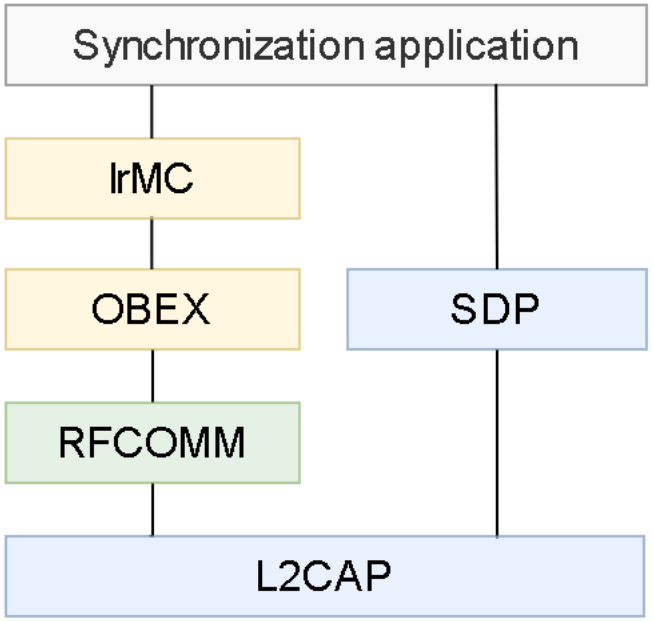


Dial-up networking

Perfiles Bluetooth: modelos de uso

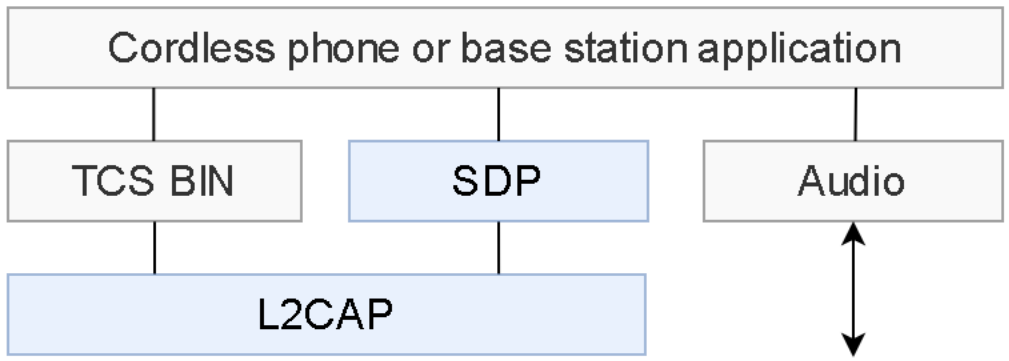


LAN access

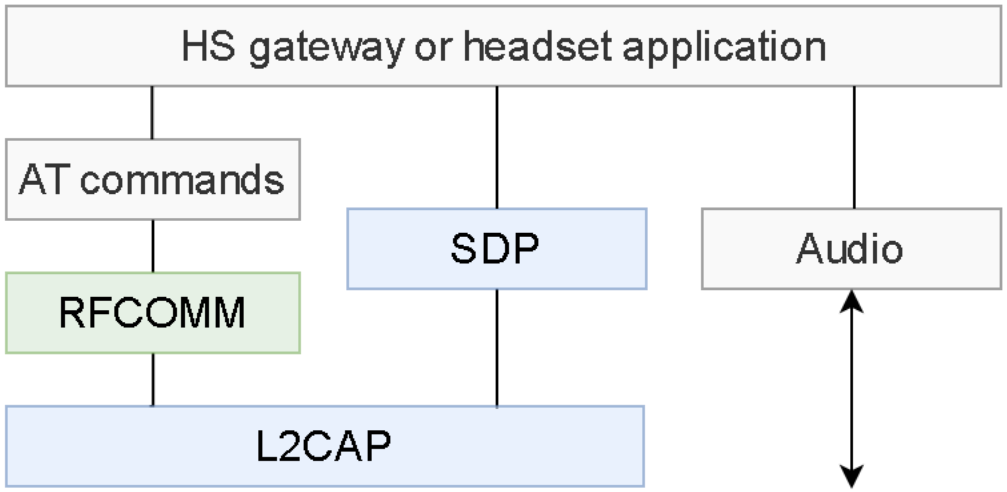


Sychronization

Perfiles Bluetooth: modelos de uso



Cordless pone and intercom



Headset

Bluetooth Low Energy (BLE)

- Consumo de potencia muy bajo
- Interesante para transmisión de tipo periódico de pequeñas cantidades de datos procedentes de sensores, como los de aplicaciones médicas o de fitness
- Posibilita la alimentación con pequeñas pilas de botón que pueden durar de 5 a 10 años
- Banda ISM (2.4 GHz)
- Potencia de salida RF similar a Bluetooth clásico
- Ahorro de energía gracias a las cortas conexiones
  - Pocos ms
  - Cantidad de datos muy reducida
- El resto del tiempo (la mayoría): sleep mode

Bluetooth Low Energy (BLE)

- Para ser descubierto, un dispositivo solo tiene disponibles 3 frecuencias
  - Ahorro de tiempo y energía ya que no hay que realizar un barrido completo de frecuencias
- Sincronización con el maestro más rápida
  - Un dispositivo disponible se conecta automáticamente al maestro que lo solicite, sin confirmación
  - Tiempo de conexión de 3 ms
  - Se utiliza para que el esclavo avise de que tiene información para enviar (por ejemplo, un dato medido por un sensor): anuncio (advertising)
- Canales de mayor ancho de banda (2 MHz)
  - Mayor índice de modulación
    - Mayor inmunidad al ruido
    - Reducción de potencia
    - Aumento del alcance

Bluetooth Low Energy (BLE)

- Menos tipos de paquetes y mensajes de control de conexión
- Menos perfiles (aunque algunos nuevos, por ejemplo, para telemedicina)
- Características comunes con Bluetooth clásico
  - Espectro ensanchado con saltos en frecuencia (40 canales en BLE: 37 datos + 3 señalización)
  - Interfaz L2CAP
  - Mecanismos de seguridad, autenticación y encriptación
- Desventajas
  - Baja tasa de transferencia (unos 100 Kbps)
  - No se permiten scatternets (aunque el número de dispositivos esclavos es muy grande ya que las direcciones de red son de 48 bits)

Seguridad en Bluetooth

- Modos de seguridad
  - Modo 1
    - El dispositivo nunca inicia la autenticación o encriptación con un dispositivo conectado
  - Modo 2
    - El dispositivo inicia la autenticación y encriptación cuando es solicitado por aplicaciones locales de forma individual
    - La mayoría de los sistemas operativos utilizan este modo por defecto
  - Modo 3
    - El dispositivo inicia la autenticación y encriptación tan pronto se establece una conexión, y rechaza la comunicación con dispositivos no emparejados (unpaired)
    - Es el modo más infrecuente