Bluetooth

Balogh András

BME-HIT

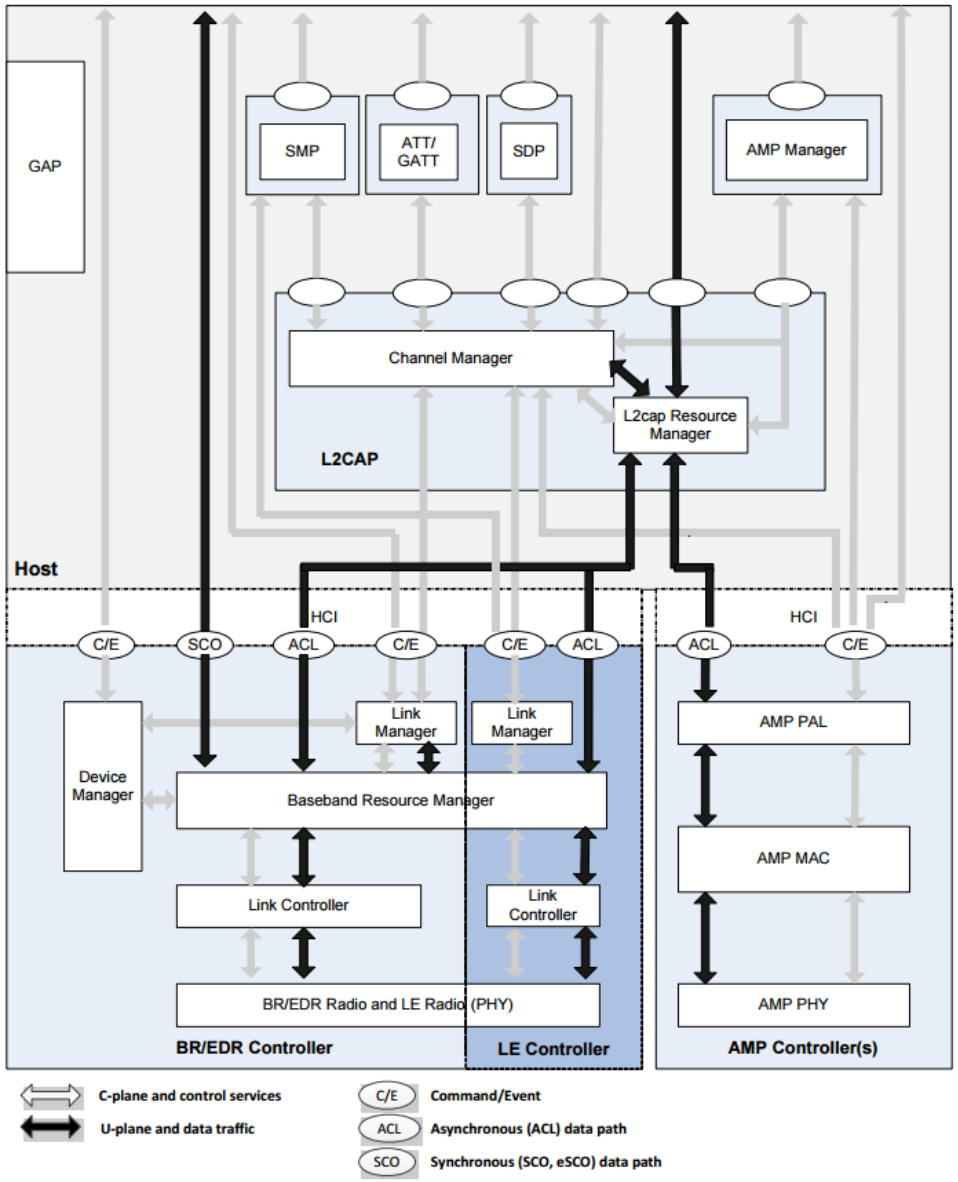
Bluetooth verziótörténet

- 1994-ben indult, 1998-ban megalakult a Bluetooth SIG
  - „Az első használható ad hoc hálózat”
  - v1.0 – 721 kbps
- Bluetooth v1.2: 1 Mbps
  - Gyorsabb felderítés és kapcsolódás
  - Adaptive frequency-hopping spread spectrum (A-FHSS)
  - IEEE 802.15.1 szabványba való beemelés
  - Flow Control and Retransmission módok bevezetése az L2CAP rétegben
- 2004 - Bluetooth v2.0: 3 Mbps
  - EDR (Enhanced Data Rate) bevezetése
    - π/4-DQPSK (2 Mbps) és 8DPSK (3 Mbps)
  - Teljesítménykímélő üzemmódok (low duty cycle)
- 2014 novemberétől ezek a verziók már nem támogatottak

Bluetooth verziótörténet

- 2007 - Bluetooth v2.1: 3 Mbps
  - Secure Simple Pairing és kötelező titikosítás
  - Párosítás OOB adatokkal (pl. NFC)
  - Újabb fogyasztáscsökkentési megoldások
  - Továbbiakban: „Hagyományos” Bluetooth
- 2009 - Bluetooth v3.0: 24 Mbps
  - 802.11 ad-hoc link bevezetése (AMP)
    - Felderítés és kapcsolódás BR/EDR interfészen
    - AMP (Anternative MAC/PHY) egységek keresése
    - Kapcsolódás és forgalom átterelése
      - Ez teszi lehetővé a nagyobb adatsebességet
- 2010 - Bluetooth v4.0: 24 Mbps
  - Bluetooth Low Energy (BLE) bemutatása
  - Az első okostelefon az iPhone 4S (2011) volt, ami támogatta
- Aktív specifikációk (2015)

Bluetooth Architektúra



Bluetooth Architektúra

- Host-specifikus architektúra blokkok
  - Logical Link Control and Adaptation Protocol (L2CAP)
    - L2CAP csatornák kezelése (létrehozás, törlés, stb.)
    - Adatfolyamok és service-specifikus információk átvitele
    - A távoli (peer) eszköz CM-évl tart fenn kapcsolatot
    - Erőforrások kezelése (Ütemezés, QoS biztosítás, stb.)
  - Service Discovery Protocol (SDP)
    - Az eszközökön definiált Service leírók felderítését teszi lehetővé
      - Leíró: Név, Alkalmazott L2CAP csatornák. Protokollok, stb.
    - Dedikált L2CAP csatornán
  - Alternative MAC/PHY (AMP) Manager Protocol
    - Távoli eszközökön található AMP-ok felderítése
      - Kapcsolódási lehetőség, adatátviteli képességek, stb.
    - Dedikált L2CAP csatornán
  - Generic Access Profile (GAP)
    - Alap Bluetooth funkcionalitások definiálása
      - Eszközfelderítési és kapcsolódási mechanizmusok
      - Biztonsági mechanizmusok

Bluetooth Architektúra

- Host-specifikus architektúra blokkok
  - Security Manager Protocol (SMP)
    - Biztonsági mechanizmusok megvalósítása
      - Kulcsok generálása, privát címek feloldása, párosítás támogatása
    - Dedikált L2CAP csatornán
    - Csak LE viszonylatban értelmezett
  - ATT/GATT
    - Attribute Protocol (ATT)
      - Szerver/kliens modellen alapuló protokollt határoz meg
      - Kérés/válasz típusú kommunikáció („tranzakció”)
      - Dedikált L2CAP csatorna felett
    - Generic Attribute Profile (GATT)
      - ATT-beli szerepekhez tartozó funkciók definiálása
    - Alapvetően LE fölé találták ezt is ki

Bluetooth Architektúra

- BR/EDR/LE-specifikus architektúra blokkok
  - Device Manager
    - GAP által definiált funkciók megvalósítása
      - Eszközök felderítése, kapcsolódás, asszociáció, stb.
      - Azaz kb. minden, ami nem adatküldéssel kapcsolatos
  - Link Manager
    - Logikai linkek felépítése, kezelés, módosítása, frissítése
      - LE-n: Link Layer Protocol (LL) segítségével
      - BR/EDR: Link Manager Protocol (LMP) segítségével
  - Baseband Resource Manager
    - Alapvetően: AZ ütemező
      - Ki, mit, mikor, melyik csatornán és hogyan küldhet…
  - Link Controller
    - L2 (MAC) adatcsomagok „értelmezése”
    - LE-n: Link Layer Protocol megvalósítása
    - BR/EDR esetén: Link Control (Baseband) funkciók megvalósítása
    - Szoros együttműködésben az ütemezővel
  - PHY
    - Csomagok küldése és fogadása a megfelelő fizikai csatornákon

Bluetooth Architektúra

- AMP-specifikus architektúra blokkok
  - AMP PAL (Protocol Adaptation Layer)
    - Interfész az AMP MAC és az L2CAP/AMP Manager között
  - AMP MAC
    - IEEE 802-nek megfelelő MAC réteg
  - AMP PHY
    - Alkalmas fizikai réteg

Bluetooth Architektúra

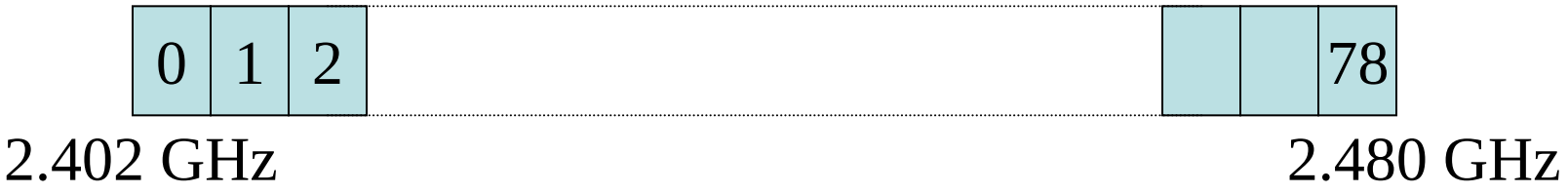
- Host-Controller Interface (HCI)
  - Inkább interfész, mint protokoll arra az esetre, ha Host és a Controller specifikus funkciók külön vannak implementálva (pl. Bluetooth Dongle)
  - A HCI szabványos felület a Host eszközök számára a szabványos BR/EDR/LE/AMP specifikus rétegek elérésére
    - A HCI-n keresztül utasíthatja a Host az alsóbb rétegeket pl. egy adott eszközhöz a kapcsolat kiépítésére, inquiry végrehajtására, hitelesítésre, teljesítmény kímélés aktiválására, stb.
    - Az alsóbb rétegek válaszolhatnak ezen utasításra
- Controllerek „felett” értelmezhető alapvető logikai transzportok
  - Asynchronous Connection-oriented Logical Transport (ACL)
    - Aszinkron, kapcsolat-orientált adatátvitelhez
  - Synchronous Connection-Oriented (SCO, eSCO)
    - Szinkron, kétirányú, kapcsolat-orientált adatátvitelhez
  - Commands/Events (C/E)
    - Parancsok, válaszok, események aszinkron jelzéséhez
      - Kvázi a HCI interfész (de mégsem teljesen az)
    - LE, Broadcast jellegű adatok jellemző belépési és kilépési pontja



BR/EDR Bluetooth működése

BR/EDR Bluetooth - Fizikai réteg

- 2,4 GHz-es ISM sáv
- Frekvenciaugratásos szórt spektrum (FHSS)
  - 1600 hop/s
  - 625 μs/szimbólum
  - 79 db 1 MHz-es vivő , f=(2402+k) MHz , k=0,1,..78
- Modulációk
  - Basic Rate (BR): GFSK (1 Mbps)
  - Enhanced Data Rate (EDR): DQPSK (2 Mbps), 8DPSK (3 Mbps)
- Bevezetett adási teljesítmény osztályok
  - Class 1: max. 20dBm (100mW)
  - Class 2: max. 4dBm (2,5mW)
  - Class 3: max. 0dBm (1mW)

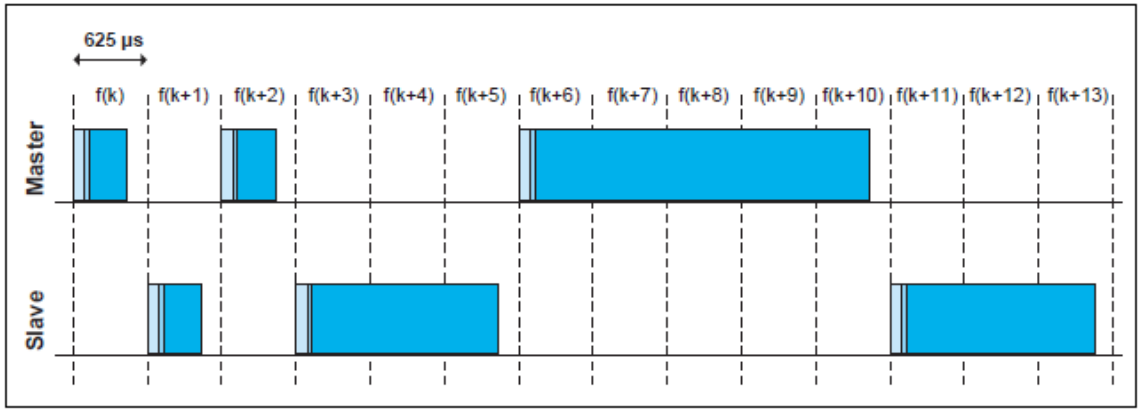


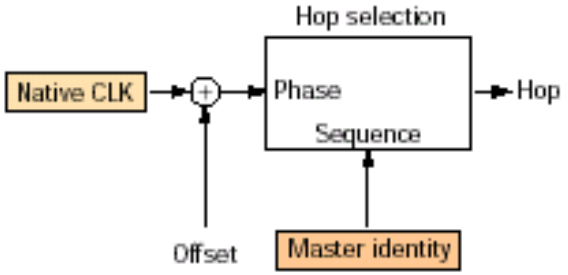
BR/EDR Bluetooth - Baseband

- Alapvető eljárásokat definiál a Bluetooth eszközök egymás közötti kommunikációjának megvalósításához
- Definiálja a(z):
  - Bluetooth linket
  - Piconet fogalmát és létrehozásának módját
  - Erőforrások megosztását egy piconeten belül
  - Csomagformátumokat
- Link Controller
  - A Bluetooth kapcsolat koordinációját végzi
- Bluetooth óra
  - 28 bites, szabadon futó, 625/2=312,5 μs-onként üt egyet, azaz hop-onként kettőt
  - 23,3 óránként ismétlődik
- Bluetooth Device Address (BD_ADDR)
  - IEEE 48 bites típusú cím, eszközönként egyedi

BR/EDR Bluetooth - Baseband

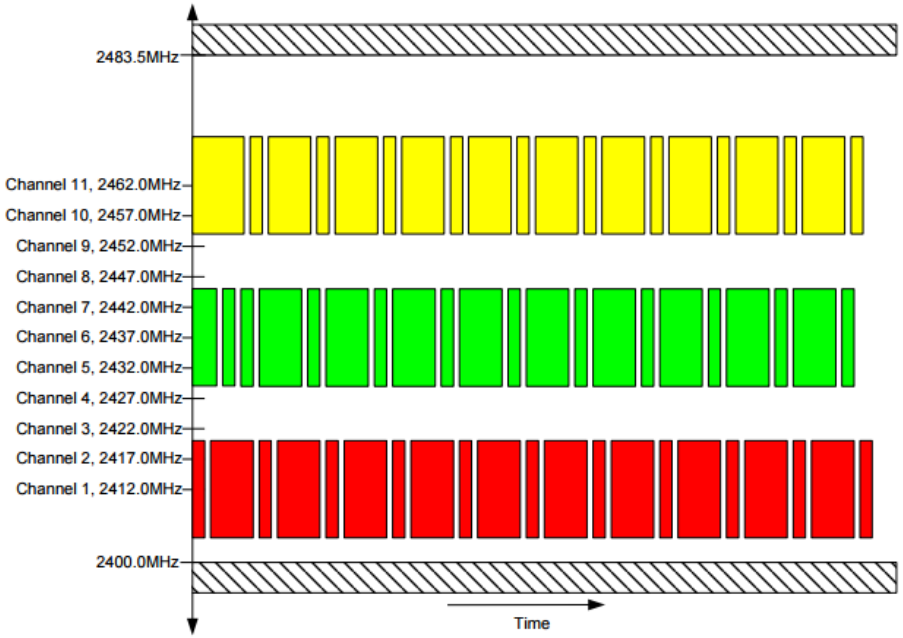
- Ad-hoc működés: Piconet
  - 1 Master és max. 7 aktív Slave
    - Parked eszközből több is lehet
  - A kommunikációt a Master szabályozza
    - Minden Slave egység hozzá igazítja az óráját
    - Basic Piconet Channel: véletlen frekvenciaugratási sorozat (79 csatorna)
    - Adapted Piconet Channel: Basic Piconet Channel min. 20 csatorna
  - A hozzáférés ezen felül időben is koordinált
    - Time Division Duplex (TDD), ha mindenkinek 1 időrése van
      - Minden páros a Masteré, páratlan a Slave-eké + 1 broadcast
      - Multi-slot csomagok miatt ez felborulhat

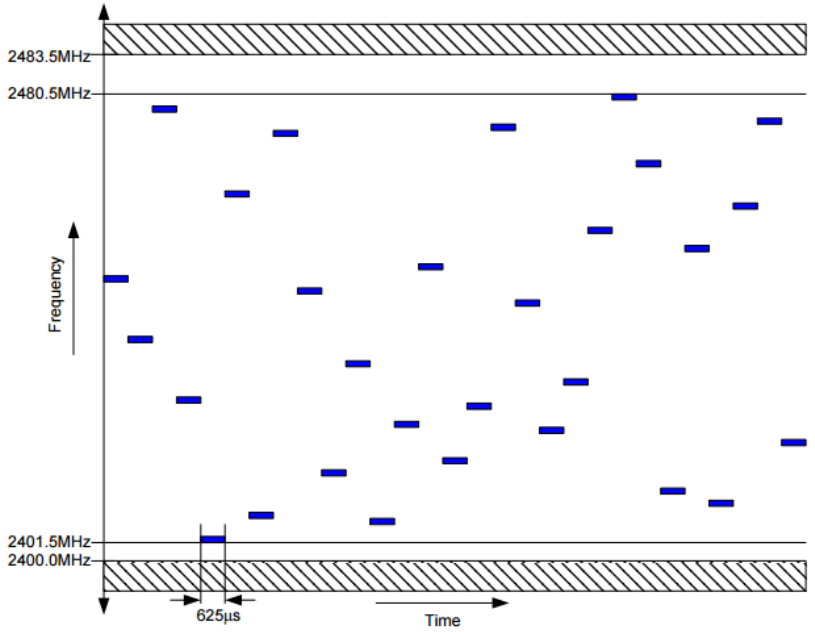




BR/EDR Bluetooth - Baseband

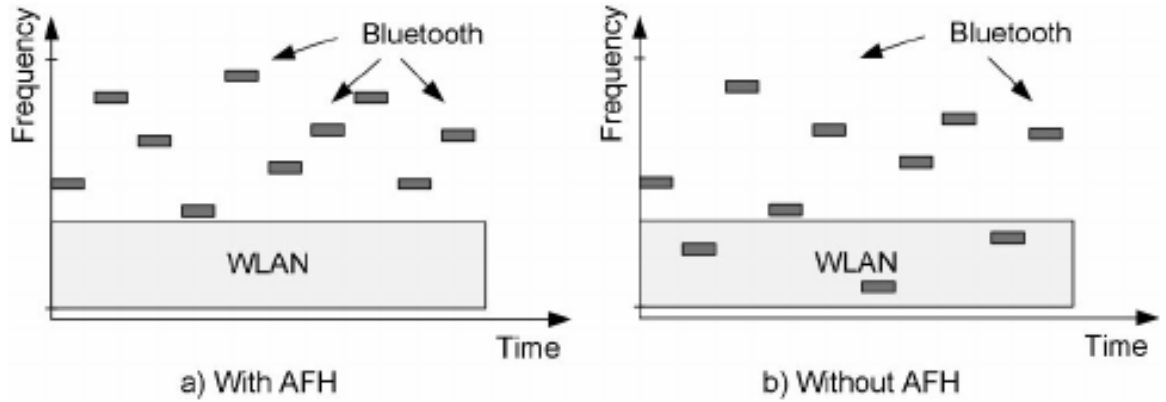
- Bluetooth FHSS vs. 802.11
  - A Bluetooth komoly interferenciaforrást képvisel
  - Ha elég jó a 802.11 spektrális kihasználtsága, akkor nagy valószínűséggel ütközni fog
    - Nincs előírva a Listen Before Talk FHSS-re a 2,4 GHz-es ISM sávban





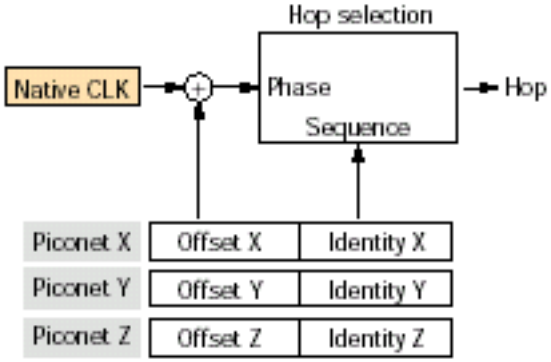
BR/EDR Bluetooth - Baseband

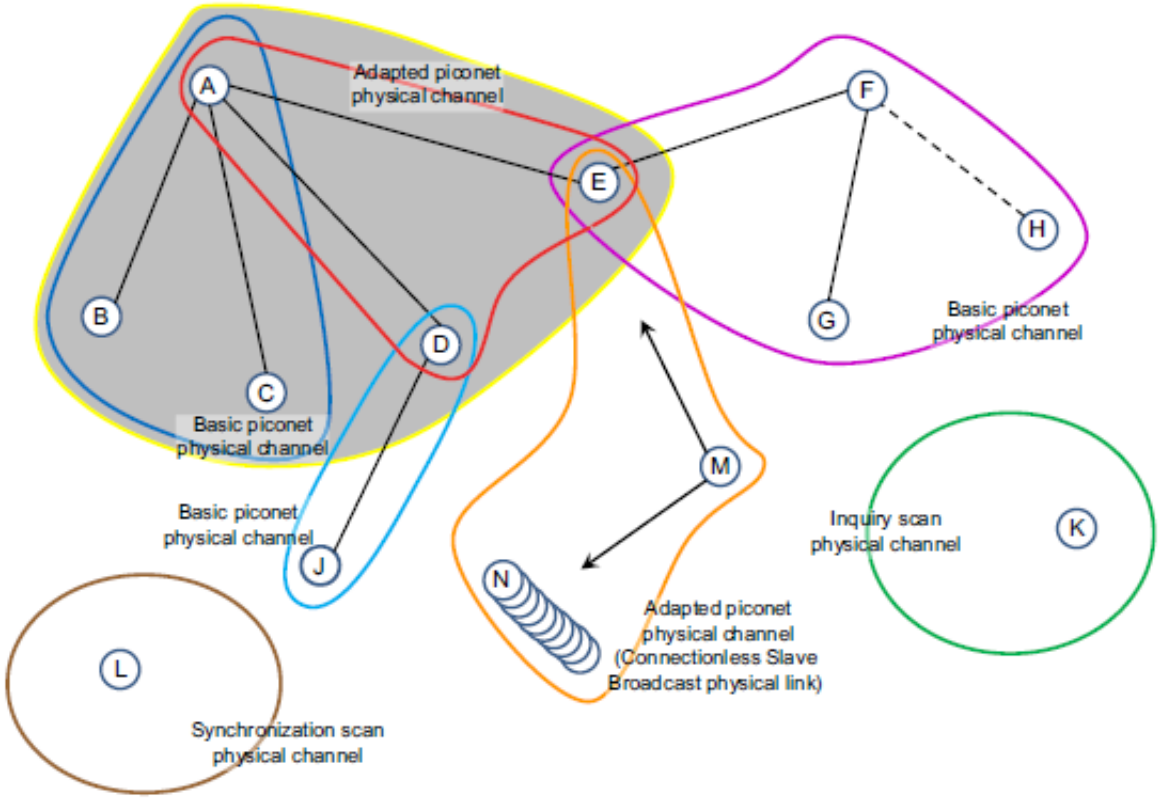
- Bluetooth FHSS vs. 802.11
  - A Bluetooth komoly interferenciaforrást képvisel
  - Ha elég jó a 802.11 spektrális kihasználtsága, akkor nagy valószínűséggel ütközni fog
    - Nincs előírva a Listen Before Talk FHSS-re a 2,4 GHz-es ISM sávban
  - Az együttélést az Adapted Piconet Channel segíti (AFH)
    - Explicite előírható, hogy mely csatornákat használja a Baseband a rendelkezésre 79 db-ból
    - Már, ha előre ismert a 802.11 konfigurációja



BR/EDR Bluetooth - Baseband

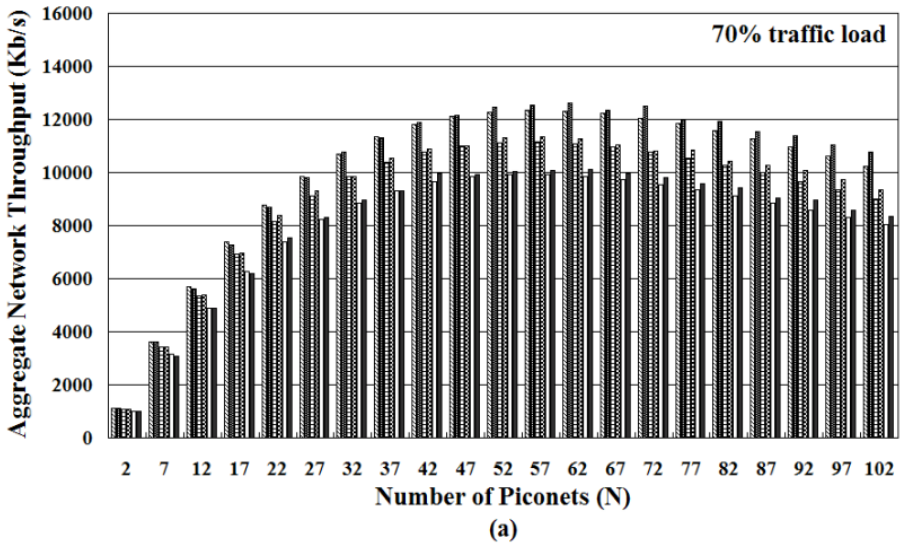
- Scatternet: több összekapcsolt Piconet
  - Olyan ugratási sorozatok szükségesek, amelyek nem ütköznek
  - Ekkor minden adott Piconet-béli hop egy ofszettel eltolható
  - Elvileg nagyobb az így elérhető throughput, de ez nem olyan egyértelmű…

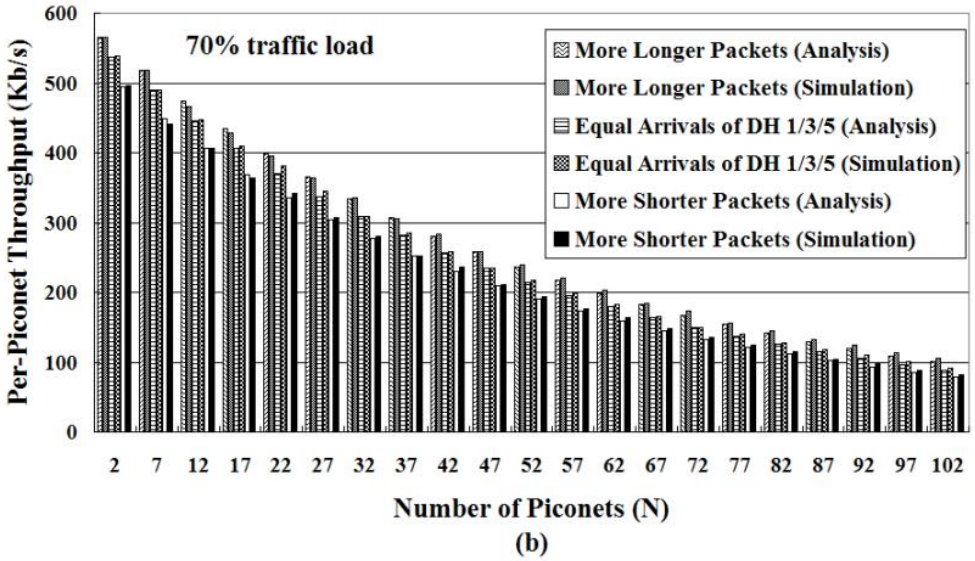




BR/EDR Bluetooth - Baseband

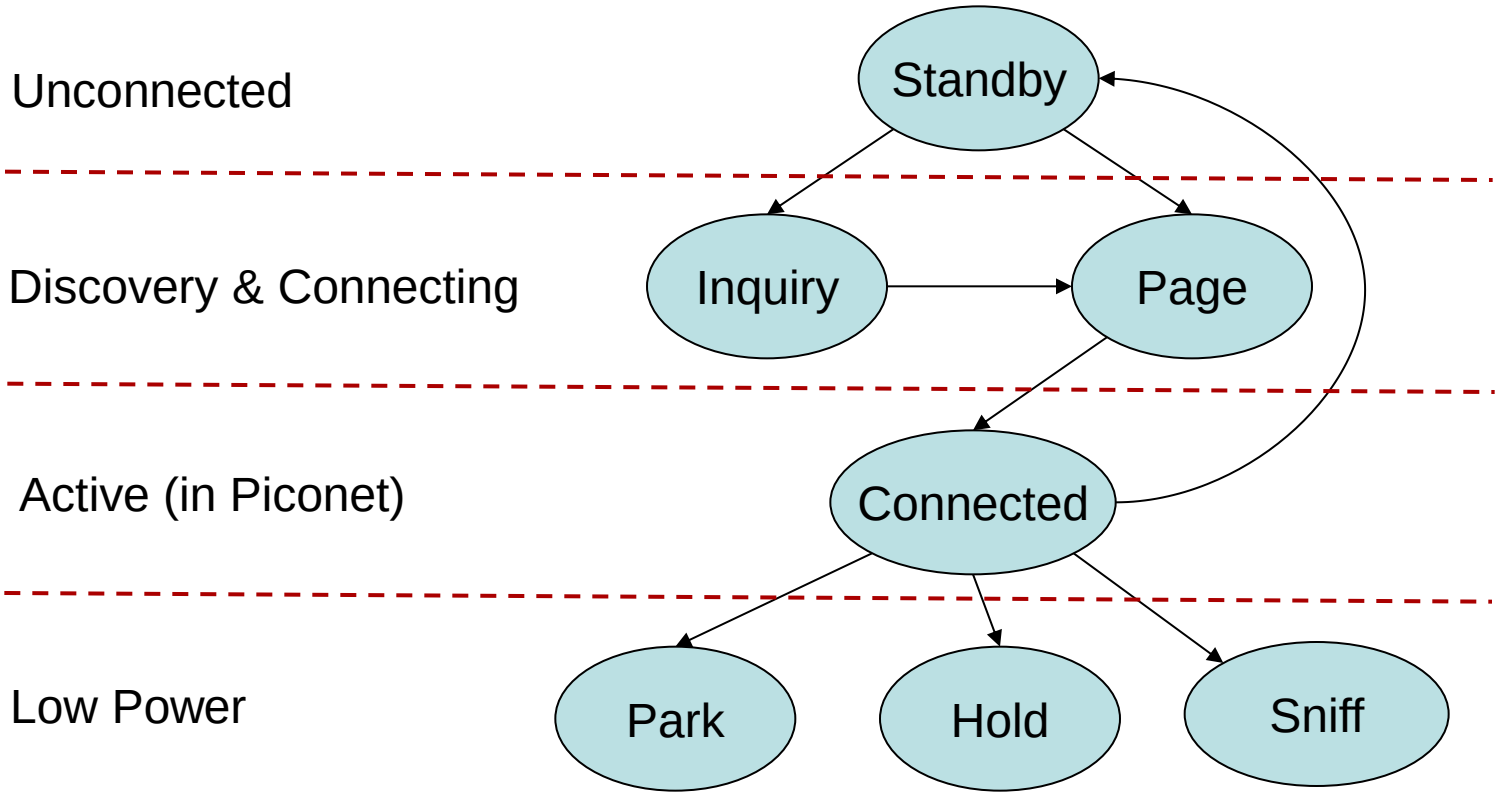
- Több független piconet egymásra gyakorolt hatása
  - Itt nem oldható meg az ütközésmentes ütemezés
  - Nincsenek szinkronban a Piconetek
    - Sok egymástól független frekvenciaugratási minta
    - Előbb-utóbb átlapolódnak
    - Így végeredményében: ALOHA





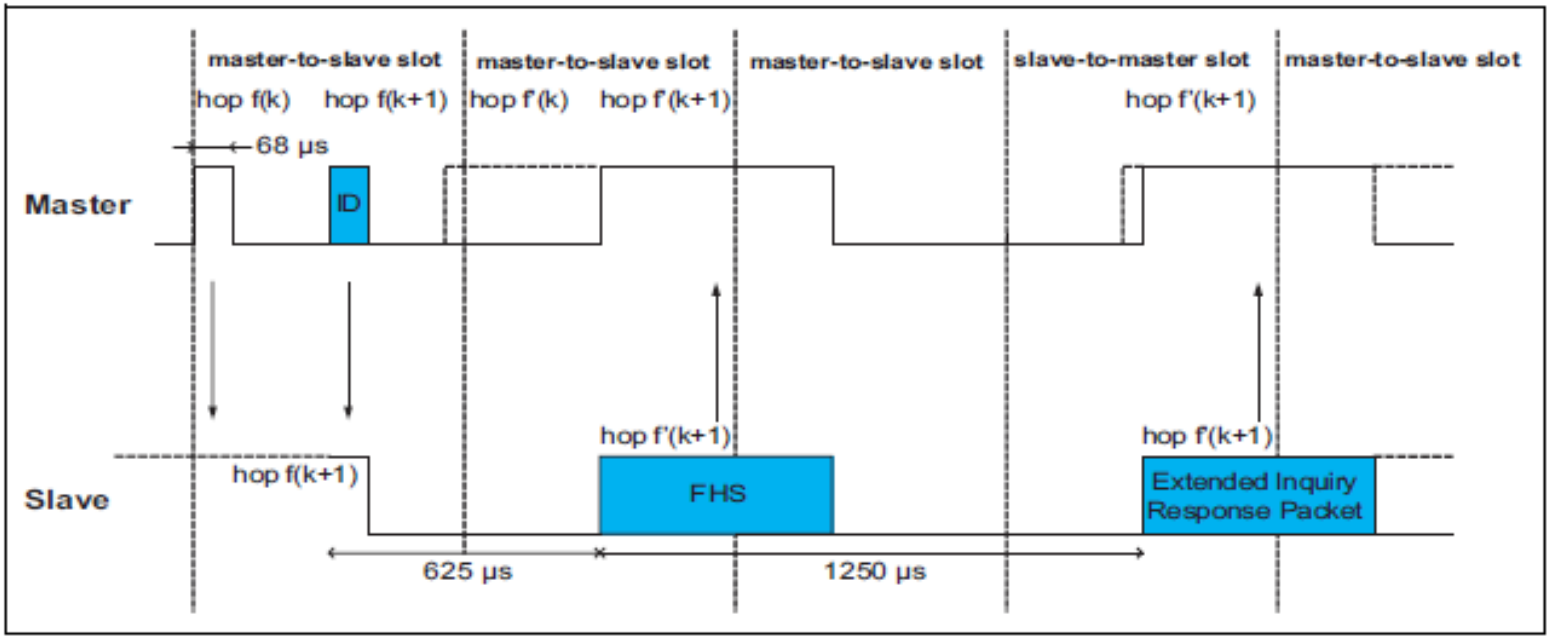
BR/EDR Bluetooth - Baseband

- Link Controller Állapotgép



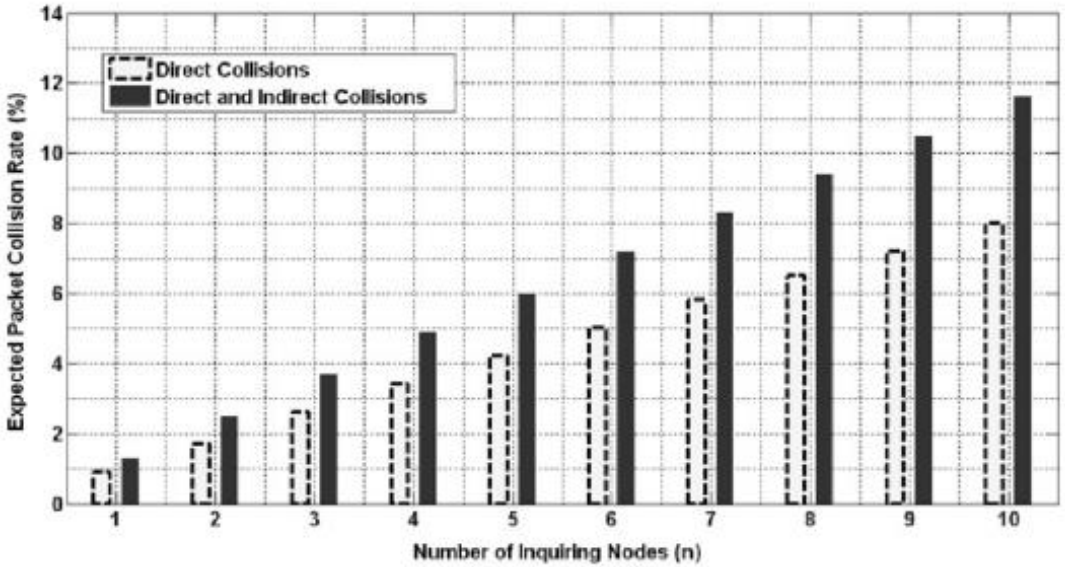
BR/EDR Bluetooth - Baseband

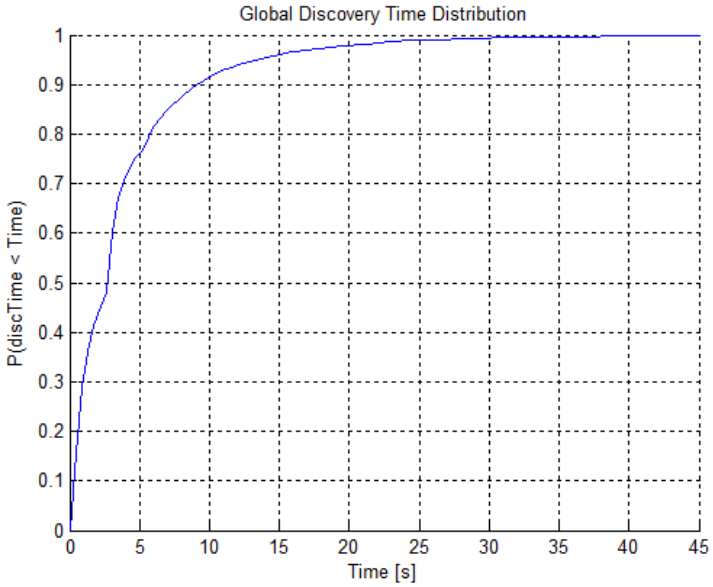
- Inquiry: Eszközök felderítése
  - Aki felderít az ID csomagokat sugároz 3200 hop/s ugrásokkal
  - Aki felderíthető és hallotta, az FHS-sel, majd EIR-rel (opc.) válaszol
  - Inquiry Scan csatornán:
    - 32 db véletlenszerűen megválasztott csatornából álló sorozat
    - Mindenki a saját órája és MAC címe alapján sorsolja
    - Ezért olyan (borzasztóan) lassú (jellemzően 10 mp, vagy több)



BR/EDR Bluetooth - Baseband

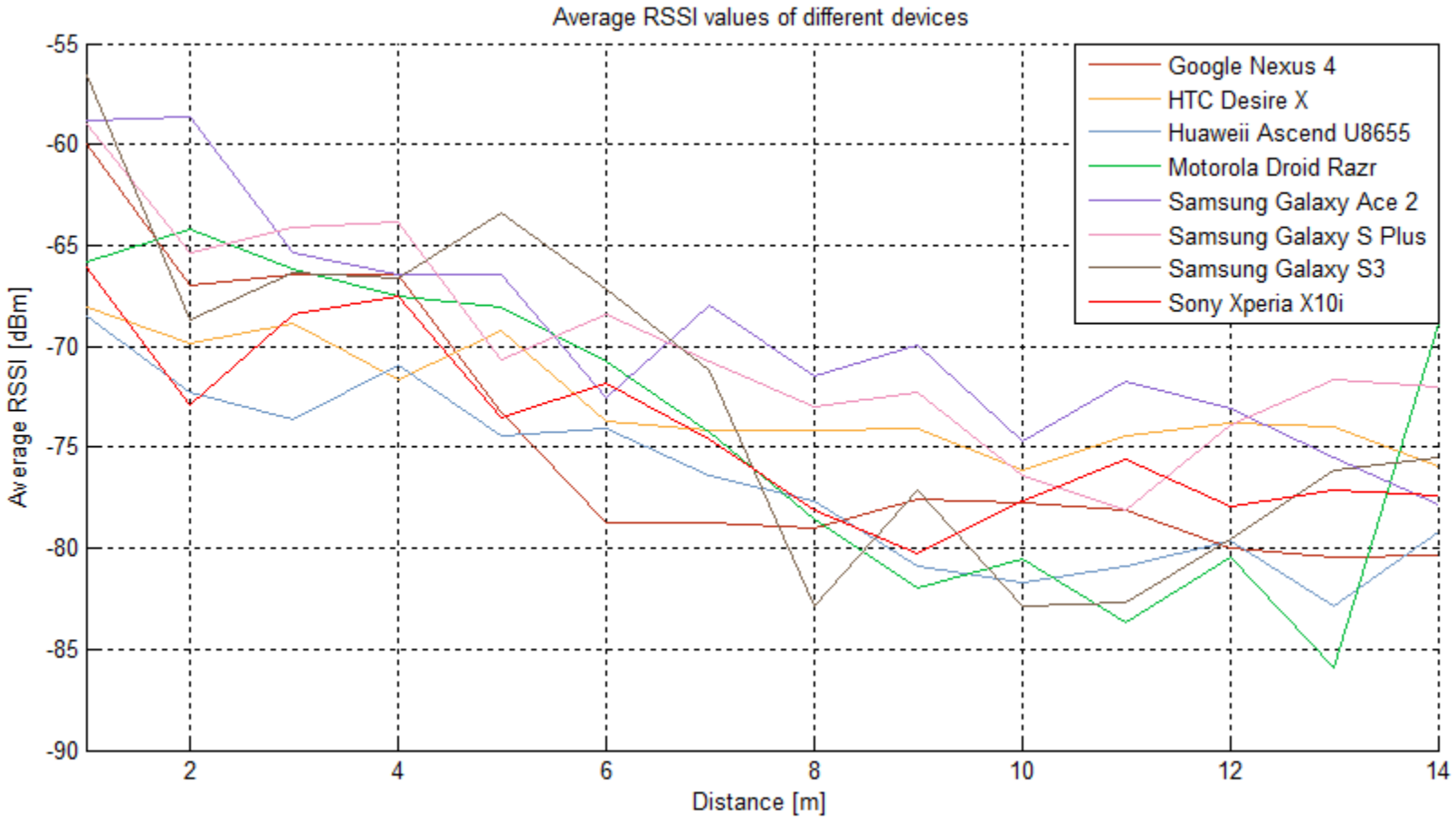
- Inquiry: Eszközök felderítése
  - Pozicionálásra többé-kevésbé alkalmas
  - RSSI mérése az FHS csomag beérkeztével történik meg
  - Ha több eszköz futtat Inquiry-t egyidejűleg az komoly interferenciát eredményezhet
    - Mérés: 9 db Android készülék egyidejűleg derít fel egyetlen másik eszközt





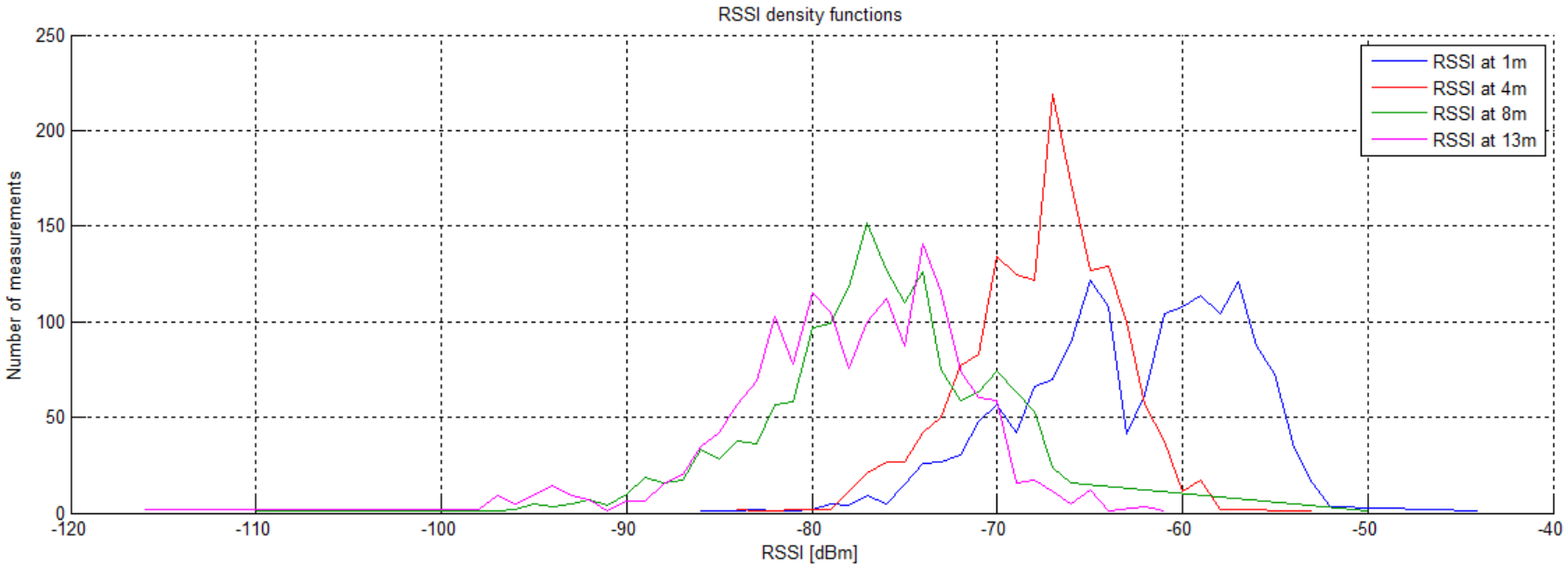
BR/EDR Bluetooth - Baseband

- Inquiry: Eszközök felderítése
  - Mérés: RSSI értékek ingadozása tipikus irodai környezetben



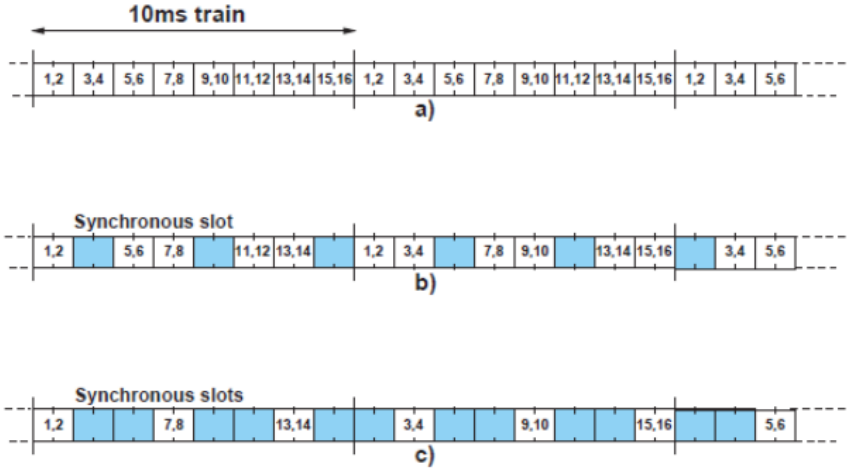
BR/EDR Bluetooth - Baseband

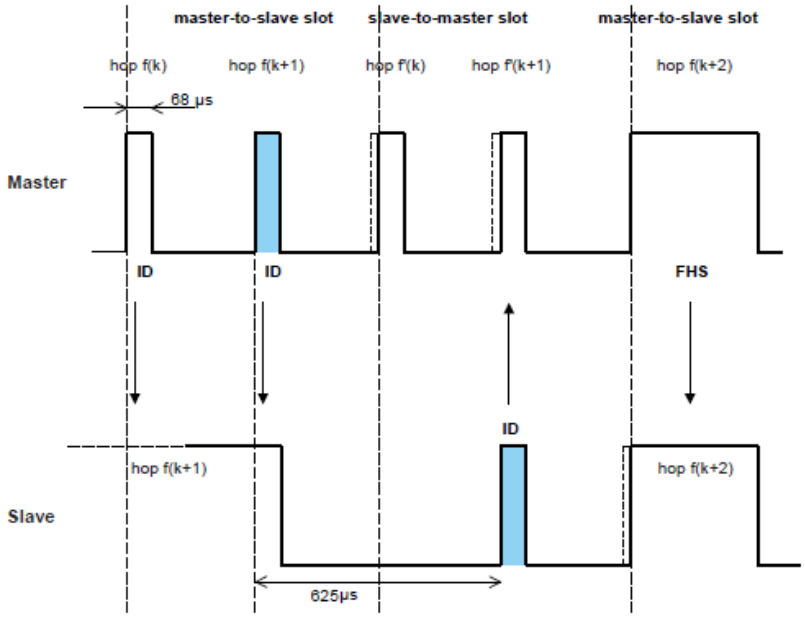
- Inquiry: Eszközök felderítése
  - RSSI értékek ingadozása
  - A reszponzivitás kritériuma mellett gyakorlatilag alkalmazhatatlanok a mobil készülékek RSSI-alapú távolságbecslésre



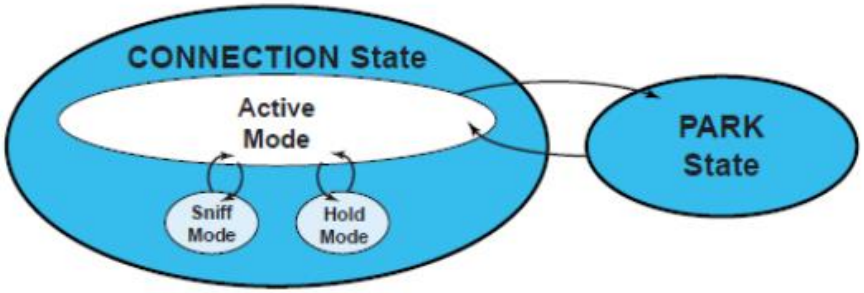
BR/EDR Bluetooth - Baseband

- Page: Eszközök bevonása a Piconetbe
  - Az Inquiry folyamat során összegyűjtött információra alapoz
    - Ebből ismert az adott eszköz órája és MAC címe
    - Megpróbálunk betalálni 3200 hops/s ugrásokkal
  - Akit bevonunk és hallotta, az ID-val válaszol
  - Ekkor létrejön a szinkron a két eszköz között
  - Ez már nem olyan lassú (2-3 mp)
  - Master FHS csomagja tartalmazza a Piconet paramétereit

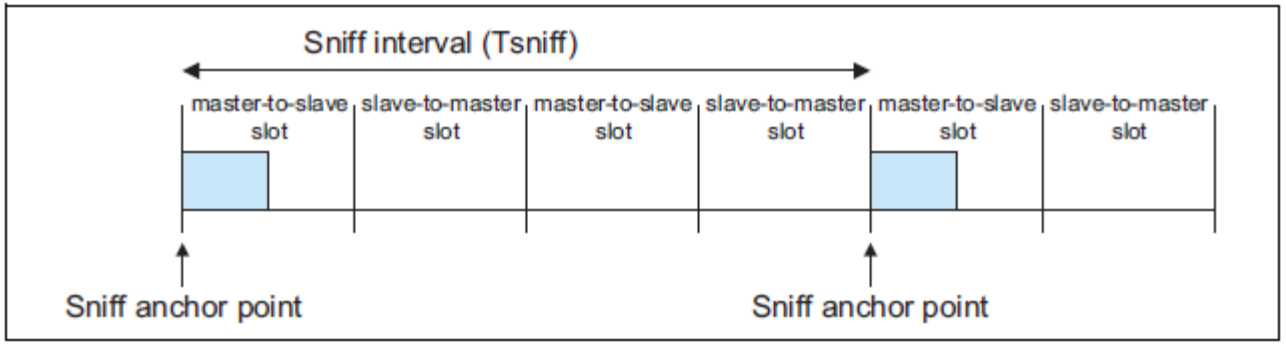




BR/EDR Bluetooth - Baseband



- Low Power állapotok
  - Sniff mód
    - Csökkentett kitöltési tényezővel működik az eszköz
    - Minden n. Master slotban ébred csak fel
    - Csak ACL linkek esetén használható

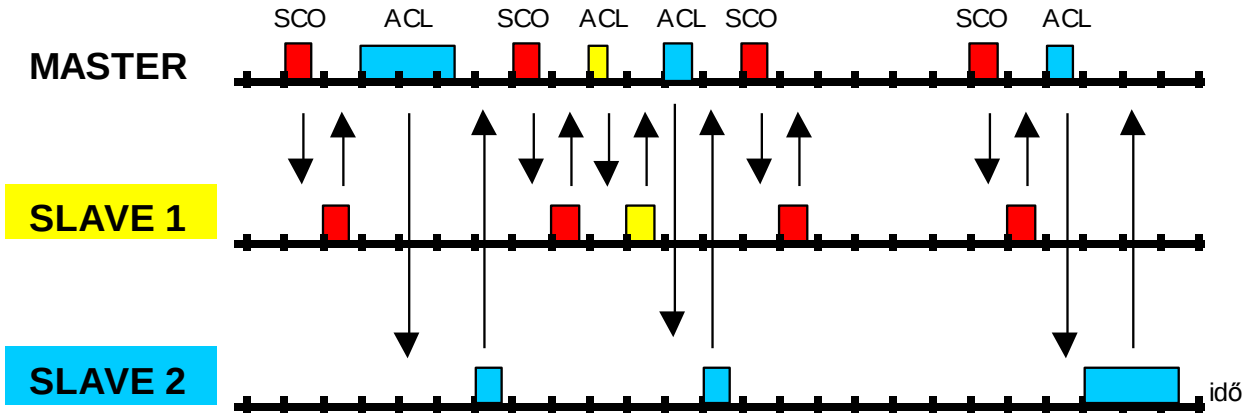


BR/EDR Bluetooth - Baseband

- Low Power állapotok
  - Hold mód
    - Az ACL linkeket felfüggeszti, az SCO linkeket megtartja
    - Akkor alkalmazzák, ha erőforrást szükséges a Slave-nek felszabadítania az egyéb tevékenységek végett
    - A Hold Timeout lejártával visszatérhet a Piconetbe
  - Park mód
    - Amikor nincs szükség a Slave aktív részvételére a hálózatban
    - Felfüggeszti az összes logikai csatornát
    - Kezdeményezhető Master és a Slave oldalról
      - A ki és a beléptetés is
    - Periodikusan fel-felébred
      - Broadcast időrésben + Szinkronizáció végett

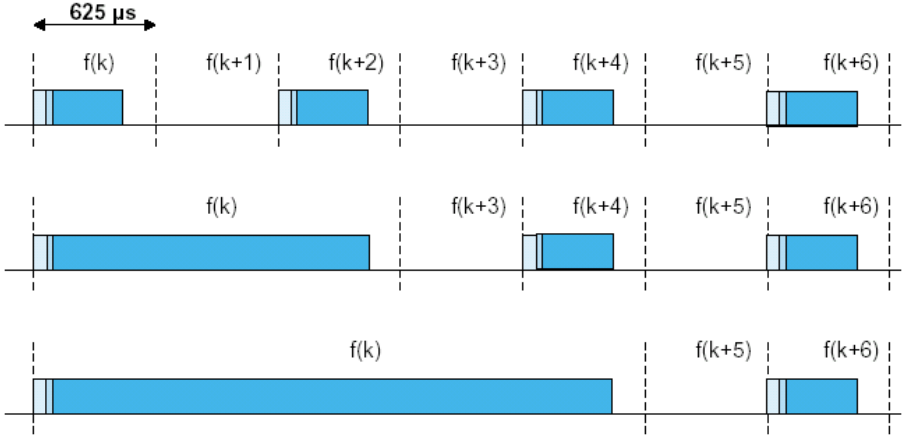
BR/EDR Bluetooth - Baseband

- Logical Transports:
  - SCO (Synchronous Connection Oriented)
    - Szimmetrikus, kvázi vonalkapcsolt
    - pont-pont kapcsolatok számára
    - fix időközönként foglalnak le réspárokat (up/down)
    - Háromféle egyréses beszédcsomagok
      - 64 kbps-os hangátvitelhez
      - NO, 2/3, 1/3 FEC lehetséges
    - ugyanakkor beszédre nincs csomagismétlés
  - eSCO (extended SCO)
    - Ugyanaz, mint az SCO, csak van újraküldés



BR/EDR Bluetooth - Baseband

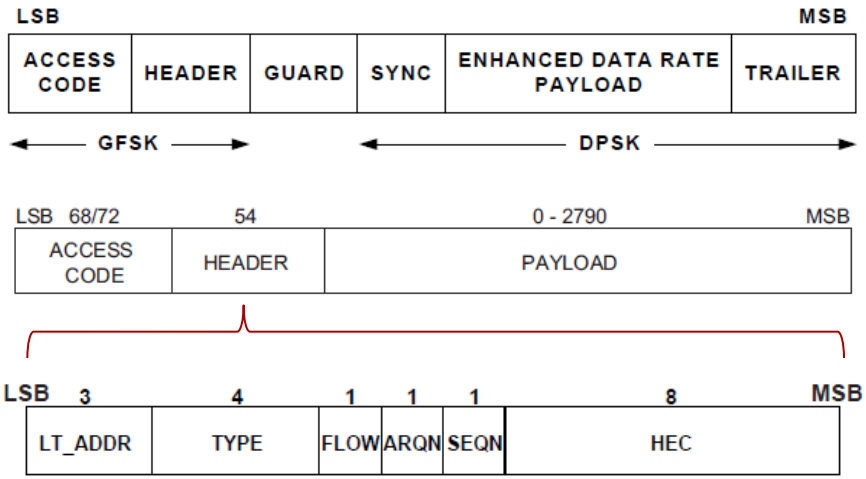
- Logical Transports:
  - ACL (Asynchronous Connection-oriented)
    - Szimmetrikus, vagy aszimmetrikus
    - Csomagkapcsolt
    - Pont-multipont börsztös adatkapcsolatok számára
    - A mester implicit (a kérés maga a downlink csomag) pollingal kérdezi le a szolgákat
    - 1-3-5 réses csomagok lehetségesek
    - NO (DHx) vagy 2/3 (DMx) FEC lehetséges
    - Adatra gyors ARQ: a vett downlink csomagot ellenőrzi a szolga és a kapcsolódó uplink csomagban jelzi ha hibát talált.



Type	Symmetric (kbit/s)	Asymmetric (kbit/s)	
DM1	108.8	108.8	108.8
DH1	172.8	172.8	172.8
DM3	256.0	384.0	54.4
DH3	384.0	576.0	86.4
DM5	286.7	477.8	36.3
DH5	432.6	721.0	57.6

BR/EDR Bluetooth - Baseband

- Csomagformátum
  - Access Code (68/72 bit)
    - Minden fizikai csatornára egyedi
    - Tartalmazza a preambulumot
  - Header (54 bit) – 1/3 FEC
    - LT_ADDR (3 bit)
      - Logical Transport Address
      - Aktív Slave-et azonosít
    - Type (4 bit)
      - Az alkalmazott csomag típusát határozza meg
    - Flow (1 bit)
      - Torlódásvezérléshez (ha megtelt az inputbuffer, Flow=0-val leállítható)
    - ARQN (1 bit)
      - Acknowledgement Indication (ACL transzport esetén)
    - SEQN (1 bit)
      - Adatstream sorrendezéséhez
    - HEC (8 bit)
      - Header Error Check (CRC a fejlécre)



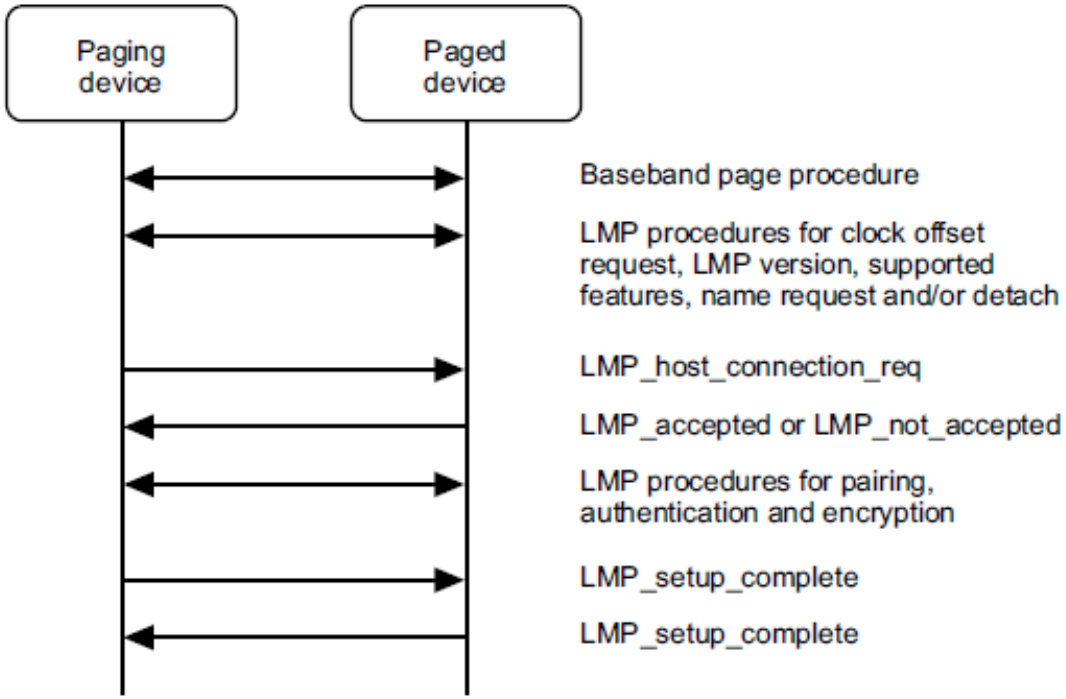
BR/EDR Bluetooth – Link Manager

- Két link menedzsment entitás között teremt kapcsolatot
  - Segítségével állíthatók be a Bluetooth linkek
- Tranzakció alapú
- Feladatok:
  - Távoli (peer) eszköz képességeinek felderítése
  - Teljesítmény kímélő üzemmódok, Biztonság, QoS
- LMP PDU Csomagformátum
  - TID (1 bit): a tranzakció kezdeményezőjének azonosítója (1, ha Master és 0, ha Slave)
  - OpCode: az LMP_PDU azonosítója és típusa
  - az LMP_PDU magas prioritású, akár az SCO csomaggal szemben is preemptív
  - 2/3 FEC kódolással ellátva

LMP PDU with 7 bit OpCode

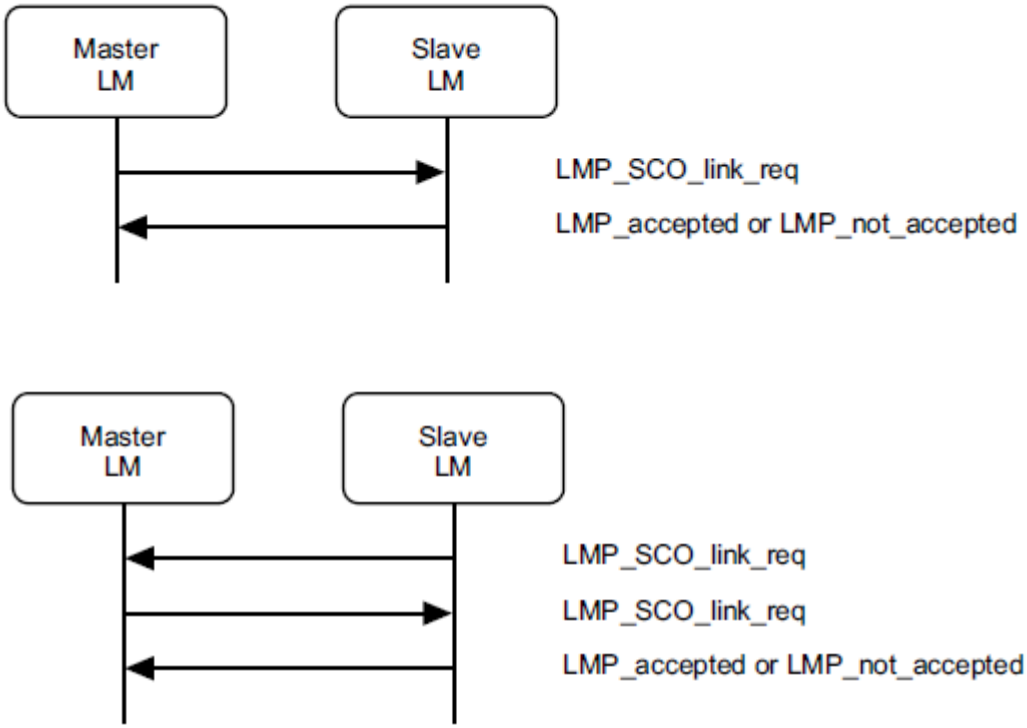
BR/EDR Bluetooth – Link Manager

- Példa: Paging procedúrát követő üzenetváltások
  - A kapcsolódást követően rendelkezésre áll egy ACL
  - Minden jelzésüzenet ezen közlekedik
    - Ezt ACL-C (al)típusú transzportnak nevezik
  - Támogatott Feature-ök: 140 bites maszk



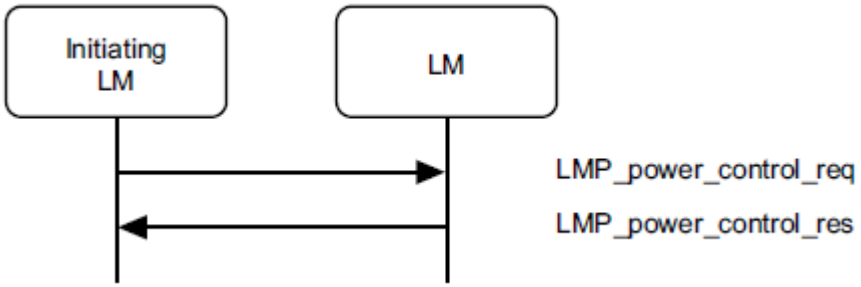
BR/EDR Bluetooth – Link Manager

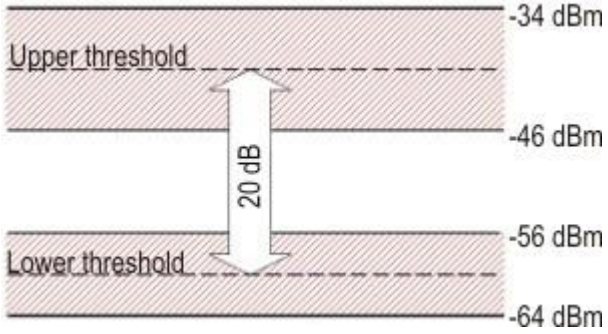
- Példa: SCO logikai transzport felépítése
  - Master és Slave is kezdeményezheti egyaránt



BR/EDR Bluetooth – Link Manager

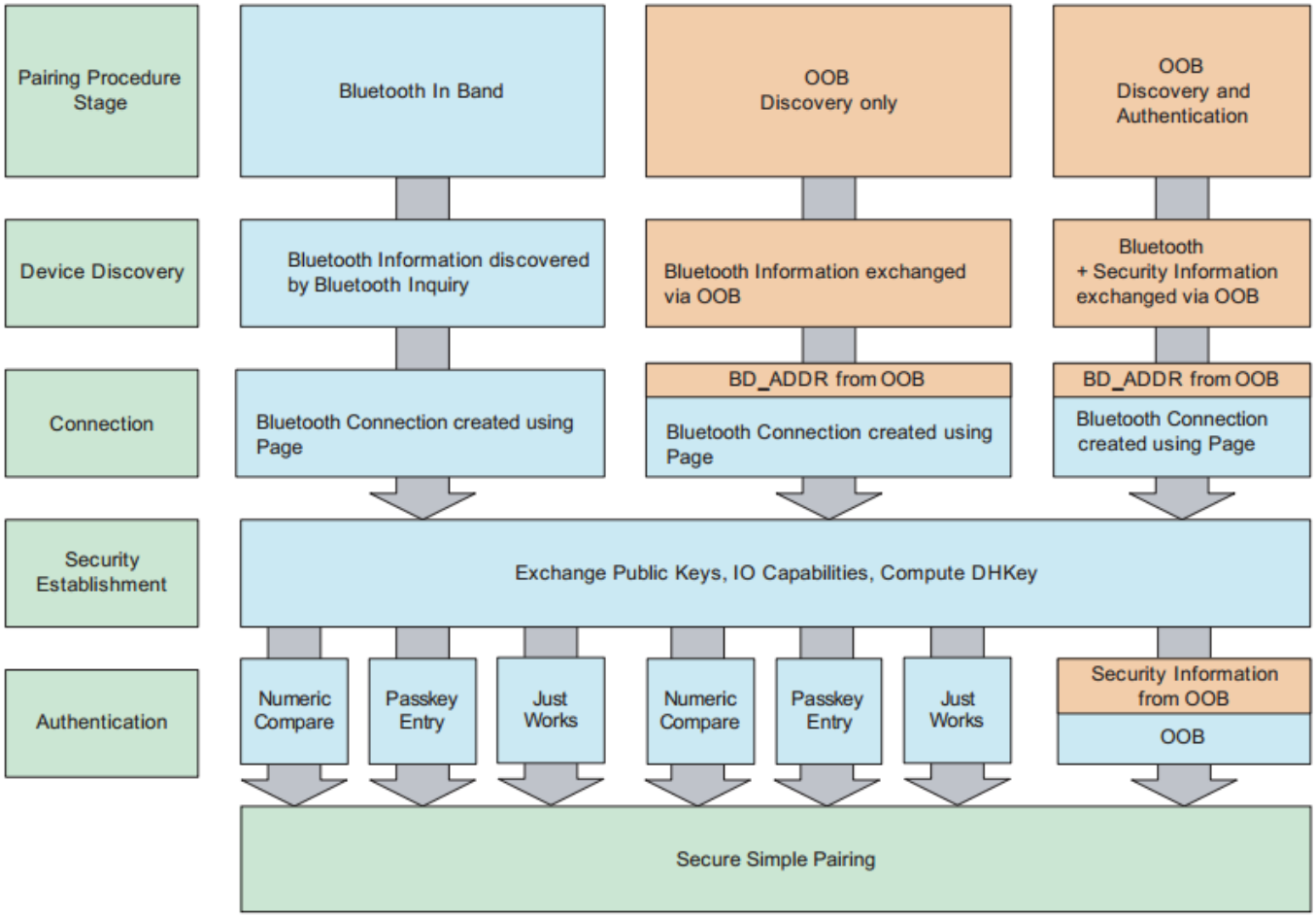
- Példa: Adaptív teljesítményszabályzási mechanizmus
  - Master és Slave is kezdeményezheti egyaránt
  - Célja: Az adási, és így a vételi teljesítmény egy bizonyos GRPR (Golden Receive Power Range) zónában tartása
    - Kevesebbet fogyaszt
    - Kisebb zavarást képvisel





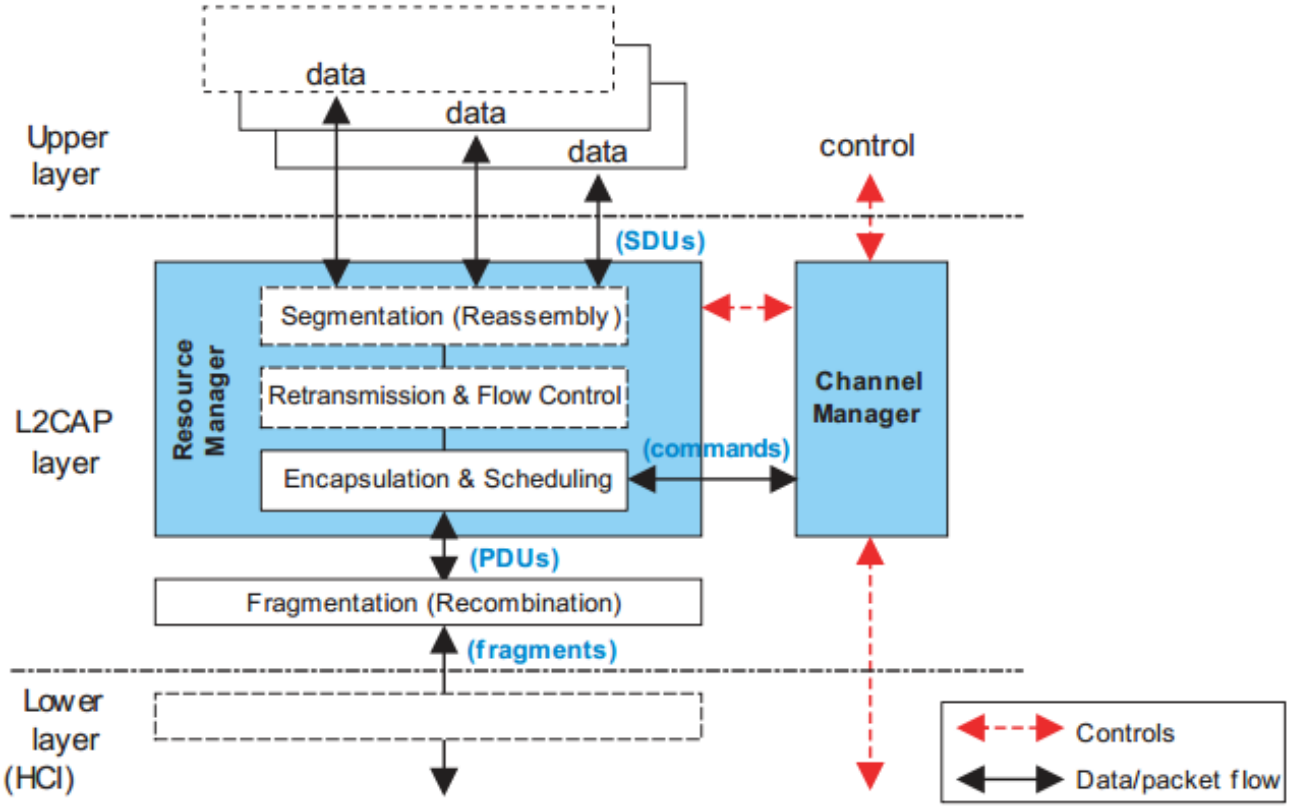
BR/EDR Bluetooth – Link Manager

- Párosítási mechanizmusok
  - Autentikáció (MITM) és a link titkosítás (Passive Eavesdropping)



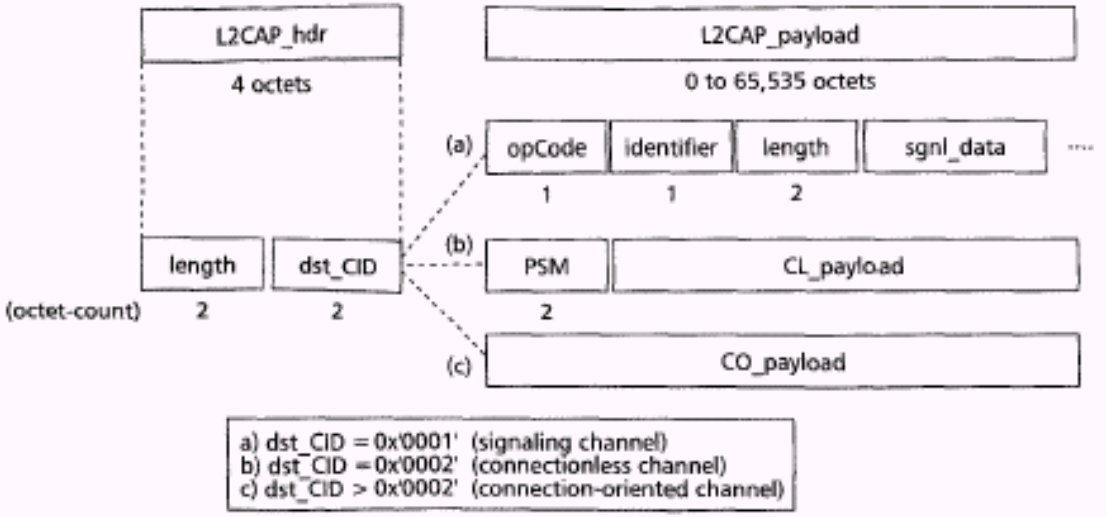
Bluetooth – L2CAP

- Elrejti az alsóbb rétegek Bluetooth specifikus jellemzőit a felsőbb rétegek elől és csomag szintű illesztést biztosít a felsőbb rétegek számára.
  - Itt tűnik el a mester-szolga viszony
- Az L2CAP csomagok jóval nagyobbak lehetnek, mint a Baseband csomagok, ezért szegmentálásra lehet szükség



Bluetooth – L2CAP

- Az L2CAP forgalom kétféle logikai csatornán zajlik
  - A csatorna végpontokat egy Channel ID (CID) azonosítja
  - Connectionless (CL), CID=0x'0002'
    - Egyirányú
    - Nincs jelzéscsatorna
  - Connection oriented (CO), CID>0x'0002'
    - Kétirányú
    - Kapcsolatfelépítés szükséges
      - Jelzéscsatornát biztosít CID=0x'0001'-val mindkét végén.
      - Két eszköz között csak 1 db. jelzéscsatorna lehet.

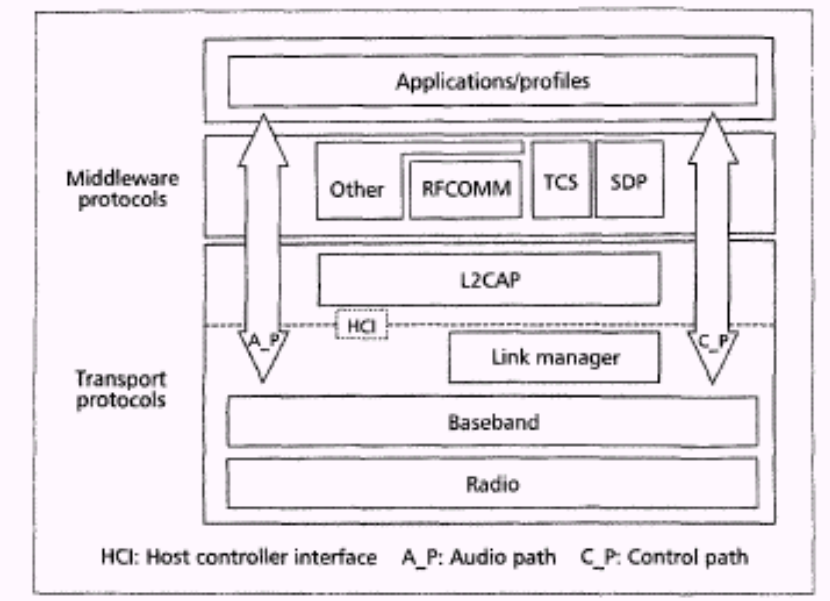


Bluetooth – L2CAP

- Csomagformátum
  - Max méret 65 535 bájt
  - (a) jelzéscsatorna:
    - opCode: a jelzési adat azonosítója
    - identifier: a kérések és válaszok párosításához
    - Length: adatmező hossza
    - sgnl_data: jelzési adata
  - (b) connectionless csatorna:
    - PSM: Protocol and Service Multiplexer
      - Segítségével lehet azonosítani a CL L2CAP csatornán multiplexált felsőbb rétegbeli vevőt
  - (c) connection oriented csatorna:
    - PSM: a kapcsolatfelépítést kérő jelzéscsomag tartalmazza, nem kell minden payloadba betenni

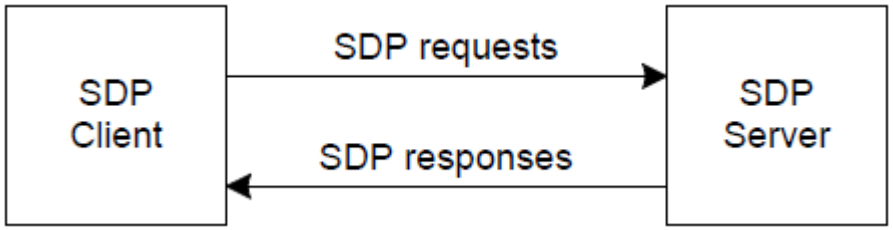
BR/EDR Bluetooth – SDP

- Eddig bejárt rétegek:
  - PHY
  - Baseband
  - Link Manager
  - L2CAP
- Efölé igazából már tetszőleges alkalmazás definiálható
  - Definiáltak is, nem is keveset
  - Az L2CAP fölé definiált rétegek az ún. Middleware Protokollok
  - Ezek alkalmazásával lehetséges az ún. profilok létrehozása
    - Profil: Olyan alkalmazás elemek, amik jól definiálható protokollegyüttesre (Service) építkeznek
  - A legtöbbet a Bluetooth SIG adaptálta, és felügyeli
- A Service Discovery Protocol (SDP) célja ezen diverzitás összefogása és menedzselhető formába öntése



BR/EDR Bluetooth – SDP

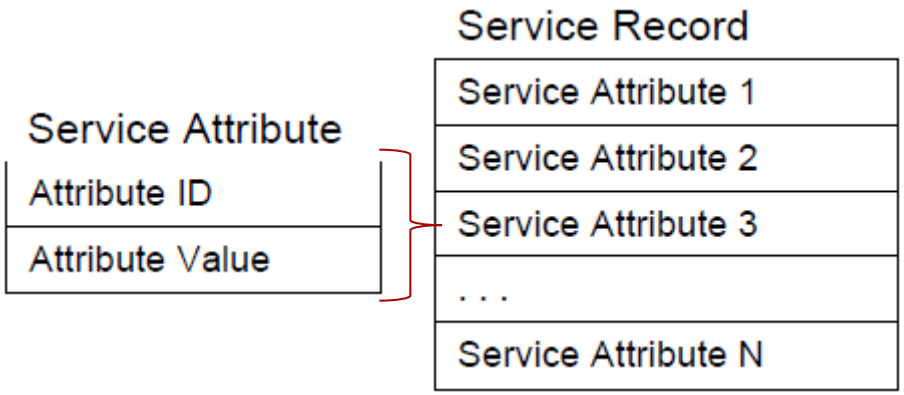
- Célja az egyes szolgáltatások (alkalmazások) protokollfüggőségeinek felderíthetővé tétele bármely fél által
  - Kérés/válasz jelleggel
- Service Registry
  - Service-ek adatbázisa
  - Service azonosítás/keresés
    - UUID-k (Universal Unique ID) segítségével
  - Hozzáférés
    - Service Record Handle (~pointer) megadásával
  - Minden Service specifikált struktúrával rendelkezik
    - Pl. SerialPort, OBEXFileTransfer, Headset, stb.



https://www.bluetooth.org/en-us/specification/assigned-numbers/service-discovery

BR/EDR Bluetooth – SDP

- SDP Service bejegyzések (Record)
  - Alaptípus: Service Attribute
  - Lehet generikus, vagy alk. Specifikus
    - Felépítés: Key (ID) + Value
  - Néhány generikus típus:
    - ServiceRecordHandle (ami alapján elérjük)
    - ServiceClassIdList (milyen más service-eket tartalmaz)
    - ServiceRecordState (a bejegyzés aktuális állapota, pl. frissült-e)
    - ServiceId (UUID, amivel azonosítható)
    - ProtocolDescriptorList (alkalmazott Protokollok)
    - IconURL
    - ClientExecutableURL
    - Stb.



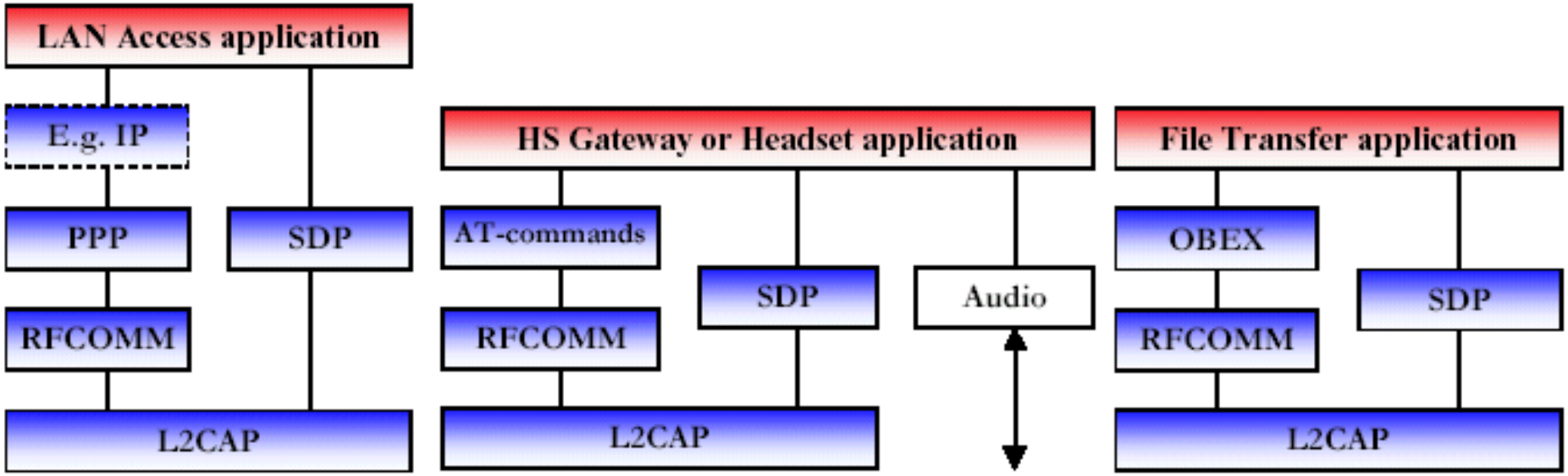
BR/EDR Bluetooth – SDP

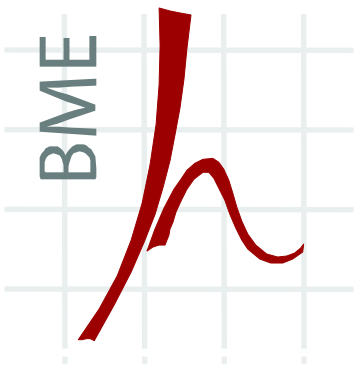
- Példa: Serial Port Profile
  - Note1: Bluetooth Assigned Numbers

Item	Definition	Type/Size	Value	AttributeID
ServiceClassIDList			Note1	0x0001
ServiceClass0	SerialPort / Note3	UUID	Note1	
ProtocolDescriptorList				0x0004
Protocol0	L2CAP	UUID	L2CAP /Note1	
Protocol1	RFCOMM	UUID	RFCOMM /Note1	
ProtocolSpecificParameter0	Server Channel	Uint8	N = server channel #	
ServiceName	Displayable text name	DataElement/ String	"COM5" / Note4	Note2

BR/EDR Bluetooth – Alkalmazások

- A protocol stack felett elhelyezkedő szoftverek együttese
  - Profilok, Protokollok, Stb.
- A szervezés gyakorlatilag a Bluetooth modul gyártójától független alkalmazásfejlesztést tesznek lehetővé





Bluetooth Low Energy

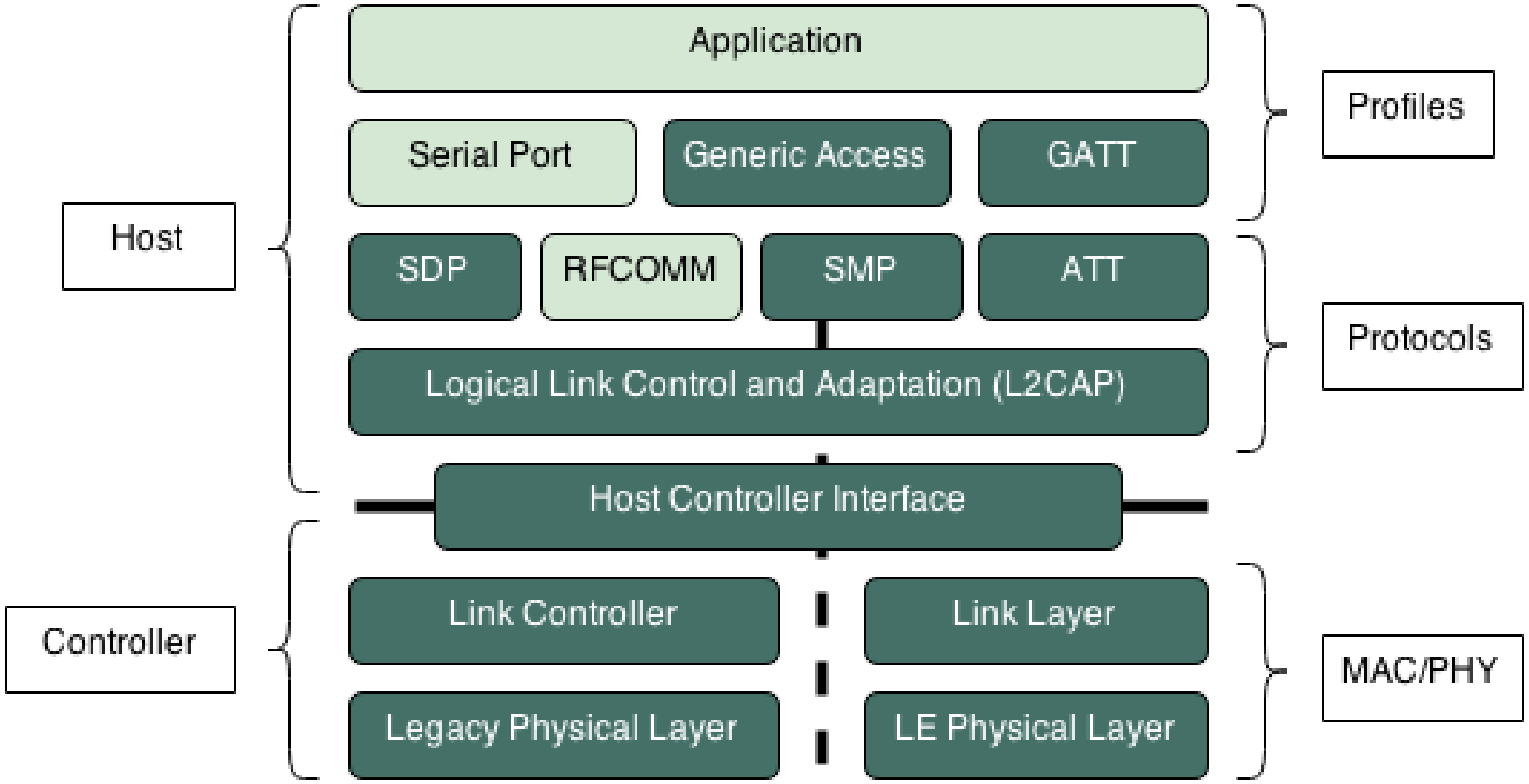
A Bluetooth LE fejlődése

- 2006 – Wibree bejelentése
  - Alacsony fogyasztású, wireless technológia
  - 2001 óta fejlesztették (Nokia)
- 2007 – v2.1+EDR, hagyományos változat megjelenése
- 2008 – A Wibree integrációja megkezdődik a szabványba
- 2009 – v3.0+HS, v2.1 bővítése ad-hoc 802.11 linkkel
- 2010 – v4.0 (+LE)
  - Bluetooth Low Energy (Smart) bemutatása
  - Dual-mode (Smart Ready) eszközök megjelenése
- 2013 – v4.1
  - BLE Scatternetek bevezetése
  - Mobile Wireless Coexistence Signaling bevezetése
- 2014 – v4.2
  - Kiterjesztett csomagméret
  - Fejlettebb Security
- 2016/2017 – v5.0
  - Nagyobb hatótávolság + egyebek

A Bluetooth LE főbb tulajdonságai

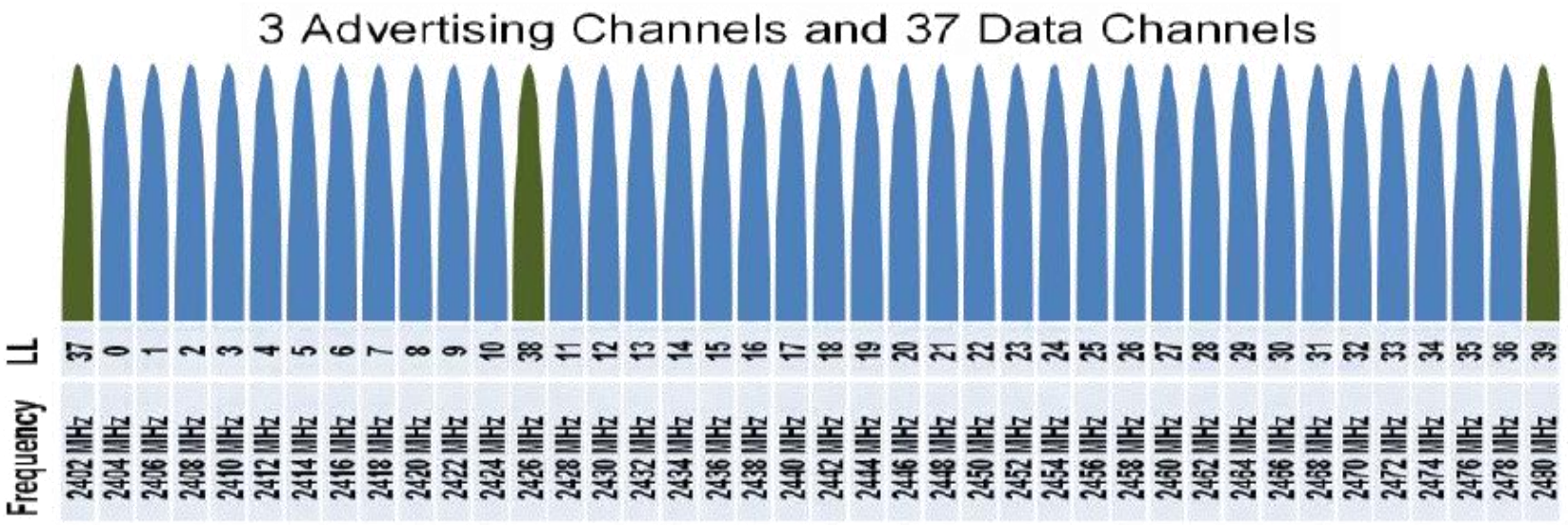
- Publikus specifikáció
  - https://www.bluetooth.org/en-us/specification
- Kisebb adatok hatékony átvitele (1 Mbps - 250 kbps)
  - Relatíve alacsony késleltetés
  - Gyors kapcsolódás (akár < 50 ms)
  - Egyszerű, robosztus stack
- Alkalmazásfejlesztési keretrendszer (GATT)
- Jól konfigurálható energiafogyasztás
  - Tipikus trade-off: Késleltetés vs. Energiaigény
- Nagy mennyiségű Slave egy piconetben (kb. 250db)
- A fontosabb mobil operációs rendszerek már támogatják
  - iOS: 2011-től (6.0)
  - WP: 2012-től (WP8)
  - Android: 2013-tól (4.3 – 18-as API szint)

Bluetooth protokoll szerkezet



BLE Fizikai réteg (PHY)

- 2,4GHz ISM sáv
- GFSK moduláció, 1Mbps jelzési sebesség
- 40 db 2 MHz-es frekvenciasáv
  - 3 db Advertising csatorna
  - 37 db Data csatorna
- Max. adási teljesítmény: 4dBm (2,5mW)

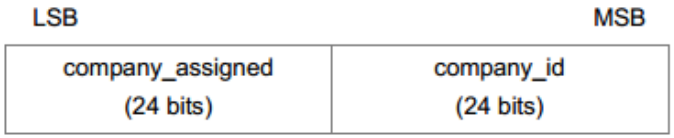


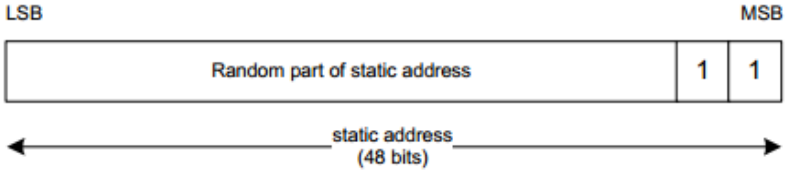
BLE Link Layer (MAC)

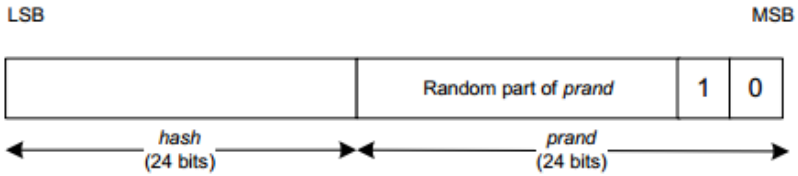
- Alkalmazott közeghozzáférési módszerek
  - FDMA (Frequency Division Multiple Access)
    - Advertising és Data (Piconet) csatornákon
  - TDMA (Time Division Multiple Access)
    - Ún. Advertising és Connection eventekben
  - Gyakorlatilag olyan, mint az FHSS, de mégsem az…
    - „Frequency hopping spread spectrum systems (FHSS) in the 2400-2483.5 MHz are in FCC 15.247(1) (iii) required to
      - a) use at least 15 channels and
      - b) when hopping, the transmission also must comply with a 0.4 second/channel maximum dwell time.
    - ETSI, FCC, JRL, stb.
      - Mindenkinél ugyanazért nem az. Helyette:
        - » FCC, JRL: Digital Modulation
        - » ETSI: DSSS

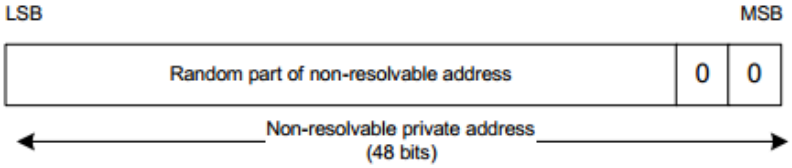
BLE Link Layer (MAC)

- Címzés
  - Publikus MAC címek:
    - Hagyományos (IEEE) MAC címek
  - Pseudo-Random MAC címek
    - Random Static
      - Véletlenszerűen sorsolt
      - Időben fix címek
    - Private címek
      - Security célokra
      - Időben változhatnak
      - Resolvable
        - » A megfelelő kulcs birtokában visszafejthető
      - Private Non-resolvable
        - » Nem visszafejthető



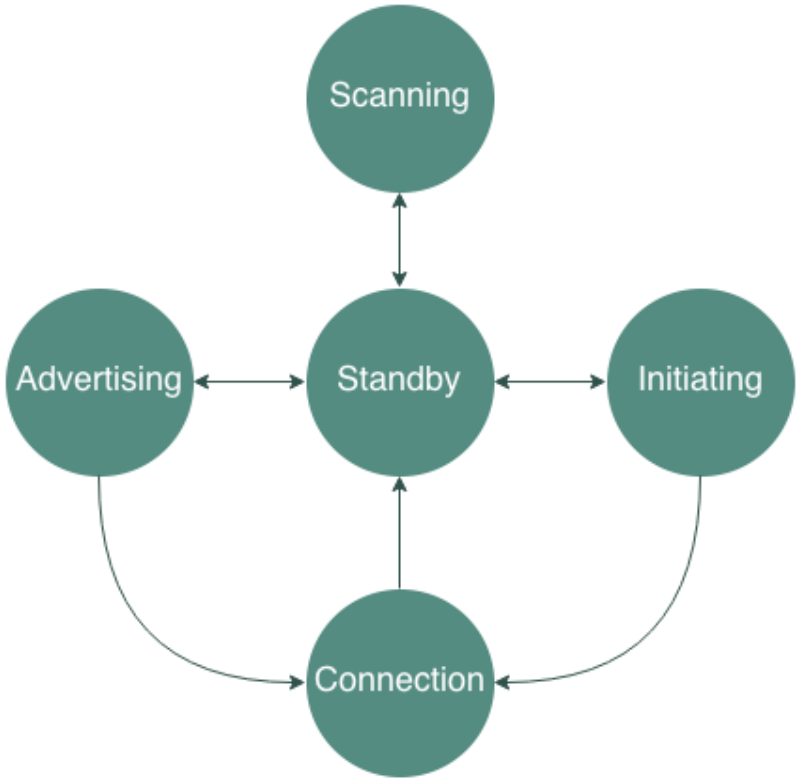






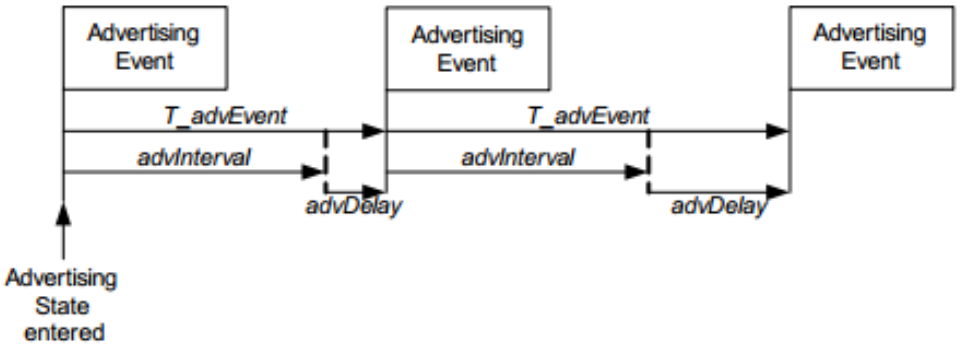
BLE Link Layer (MAC)

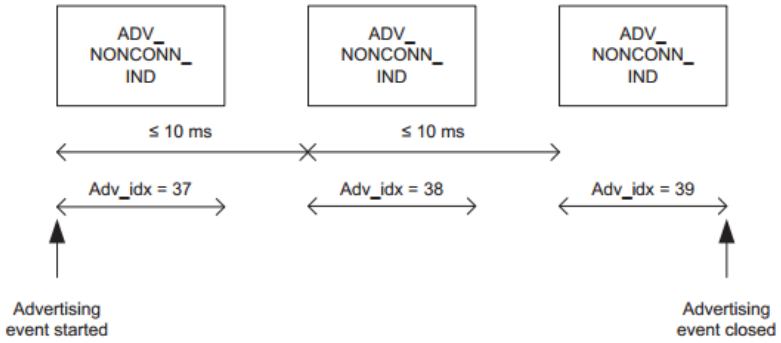
- Állapotgép



BLE Link Layer (MAC)

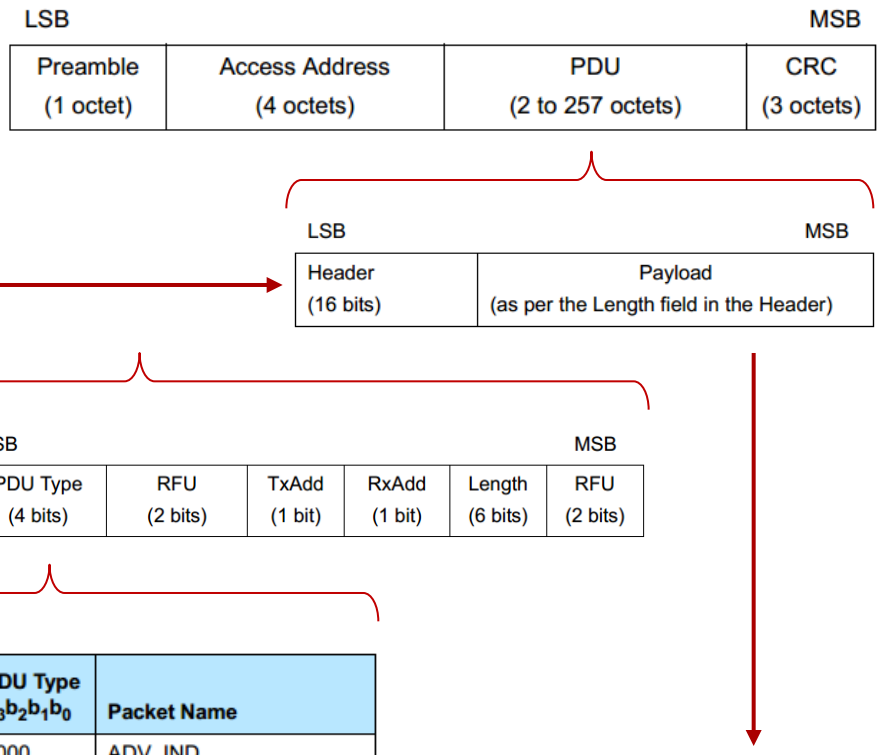
- Advertising
  - A felderíthetőség állapota
  - Hirdetmények sugárzása az Advertising eventekben
    - advInterval ≅ periodicitás > 20 [ms]
    - advDelay ∈ [0, 10] [ms]
      - Véletlenszerűen sorsolt
      - Az ütközések elkerülése végett
  - Advertising csomagok (PDU) segítségével





BLE Link Layer (MAC)

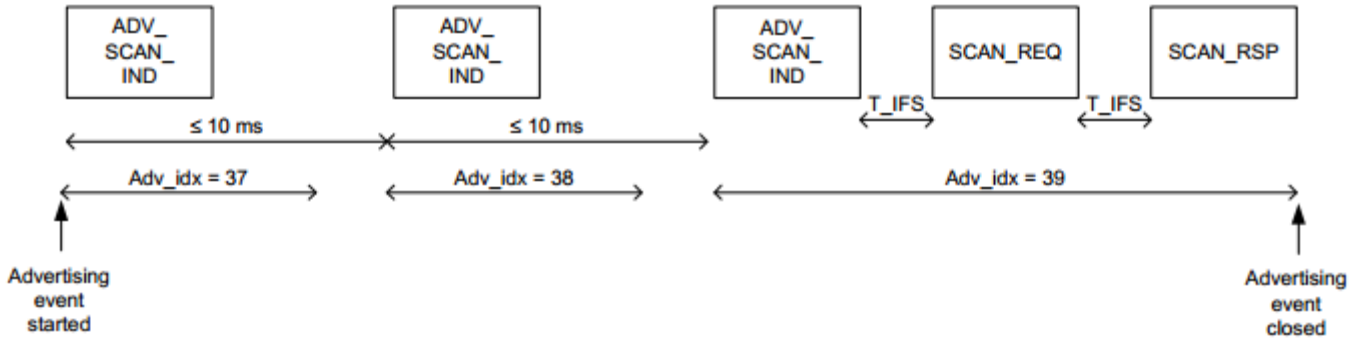
- Advertising Channel PDU
  - Link Layer keret
    - Access Address
      - Advertising csatornákon fix
      - Ez alapján dönthető el a PDU típusa (D, A)
  - Advertising Channel PDU
    - PDU Type
      - Mindegyik másra jó
    - TxAdd
      - Random-e a forráscím
    - RxAdd
      - Random-e a célcím



PDU Type $b_3b_2b_1b_0$	Packet Name
0000	ADV_IND
0001	ADV_DIRECT_IND
0010	ADV_NONCONN_IND
0011	SCAN_REQ
0100	SCAN_RSP
0101	CONNECT_REQ
0110	ADV_SCAN_IND
0111-1111	Reserved

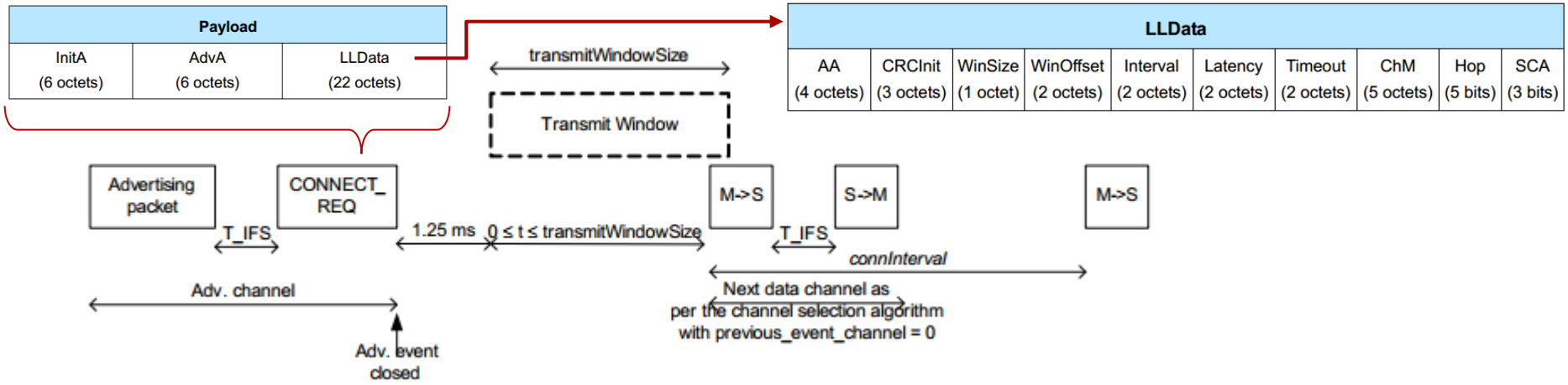
BLE Link Layer (MAC)

- Scanning
  - A felderítés alapfolyamata
    - Hallgatózás a hirdetési (Advertising) csatornákon
  - scanWindow = RX időablak mérete (egy csatornán)
  - scanInterval = periodicitás
  - Lehet aktív vagy passzív folyamat
    - Aktív, ha adott PDU típusok esetében SCAN_REQ PDU segítségével további információt szeretnénk kinyerni az eszközből
      - Ekkor a másik fél SCAN_RSP PDU-val válaszol
    - Passzív, ha nem



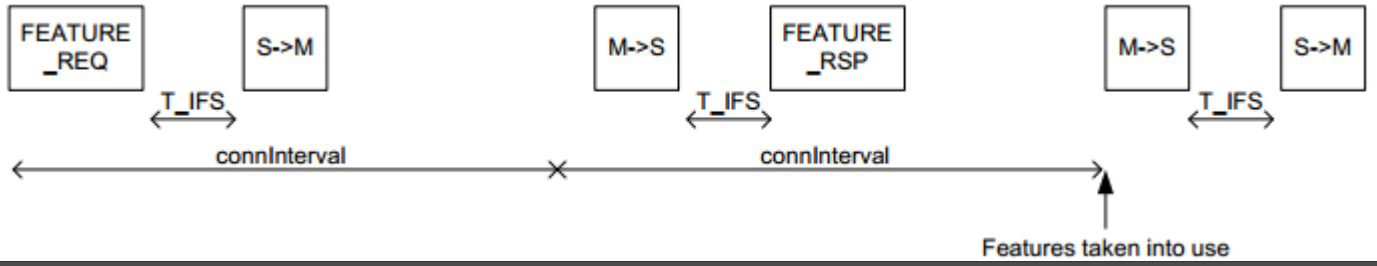
BLE Link Layer (MAC)

- Initiating
  - Kapcsolatfelépítés kezdeményezése
  - Hirdetési csatornákon CONN_REQ PDU küldése, majd Connection állapotban Master szerep
    - Transmit Window: Ekkor kezdhet el adni Masterként
    - Access Address: Master-Slave páronként egyedi
    - ChannelMap: Alkalmazott Data csatornák
    - Hop: Véletlenszerűen sorsolt ugrásszám
    - SCA: System Clock Accuracy
    - + egyéb Connection specifikus paraméterek



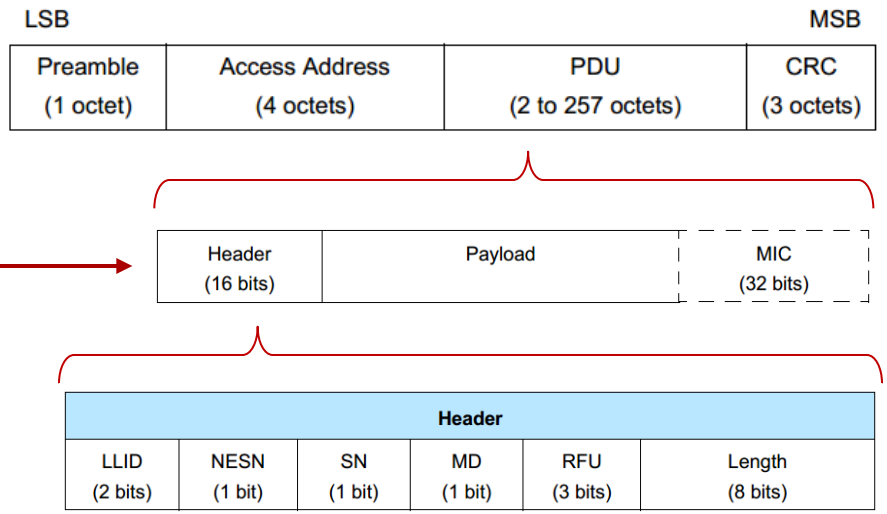
BLE Link Layer (MAC)

- Connection
  - Data csatornák és Data Channel PDU-k használata
    - Mindig Master küld először (ez adja a szinkront), a Slave „válaszol”
    - Slave-enként eltérő frekvenciaugratási minta
      - Random Hop érték a CONN_REQ PDU-ban
  - Connection eventek időzítései
    - connInterval ≥ 7.5 ms
      - Connection eventek között eltelt idő
      - Az aktuális frekvencián eddig tartózkodhat a két eszköz
        - » Ezért nem FHSS…
    - connSlaveLatency
      - A Slave max. ennyi Connection eventet hagyhat ki
    - connSupervisionTimeout
      - Ha ennyi időn belül nem érkezik válasz egyetlen Master által küldött Data PDU-ra sem, akkor bomlik a kapcsolat



BLE Link Layer (MAC)

- Data Channel PDU
  - Link Layer keret
    - Access Address
      - Ez alapján dönthető el a PDU típusa (D, A)
      - Itt már nincs MAC cím
  - Data Channel PDU
    - MIC (Message Integrity Check)
      - Aláírás (opcionális)
    - Header
      - LLID: Control Csomag (11b), kezdő darab (10b), vagy folytatás (01b)
    - NESN (Next Expected SN), SN (Sequence Number)
      - Elosztott 2 állapotváltozó bit az ACK jelzéséhez
    - MD (More Data)
      - Ha bármelyik félnek van még küldeni valója



L2CAP - HCI

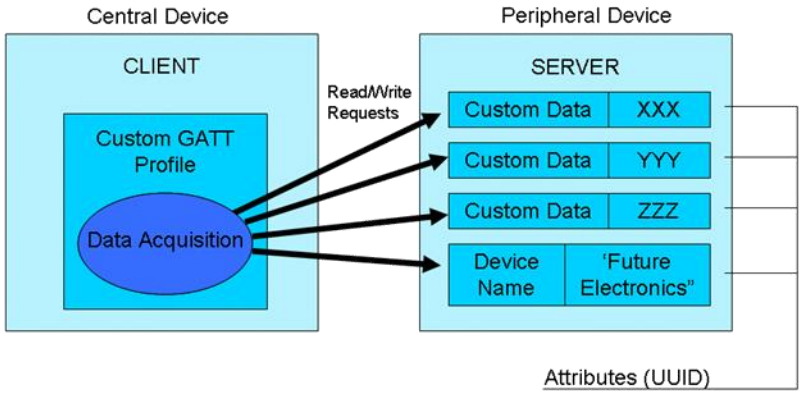
- L2CAP: Gyakorlatilag nincs változás a hagyományoshoz képest
  - Csatorna alapú absztrakció (Channel ID)
- HCI: System-on-Chip (SoC) rendszerek esetén nincs rá szükség
  - Kivéve, ha külső vezérlést végzünk (ez nem jellemző)
  - Egy sereg új Command/Event került definiálásra

ATT és SMP protokollok

- Attribute Protocol (ATT)
  - Képességek és szolgáltatások felderítése
    - Service Discovery Protocol (SDP) egyfajta általánosítása
  - Tranzakciójellegű üzenetváltások
    - RFCOMM helyett…
- Security Manager Protocol (SMP)
  - Biztonsági szolgáltatások (AES)
    - Párosítás (MITM, titkosítás)
  - Hash generálás
    - Privát MAC címek, Message Authentication Code (MIC)
  - Kulcskezelés
    - Long Term Key, Short Term Key

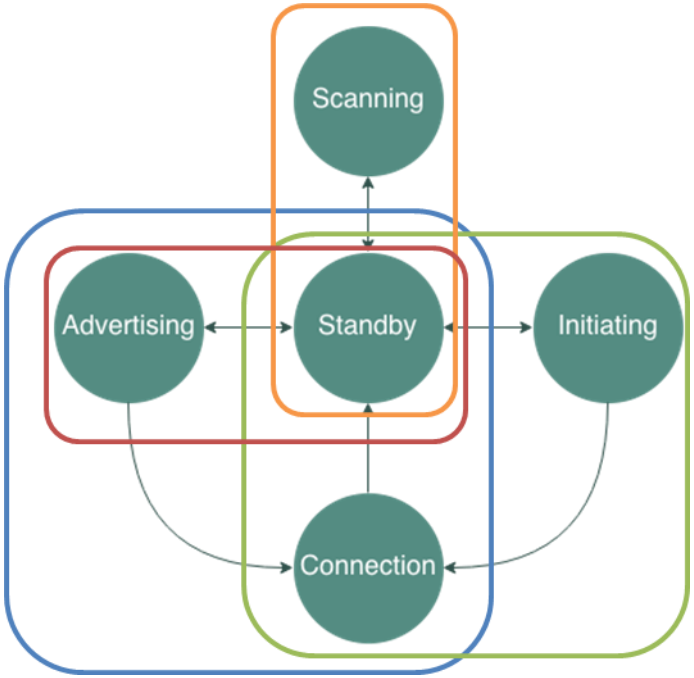
Generic Attribute Profile (GATT)

- Kliens és szerver szerepek
  - Akár egyidejűleg
- Jól definiált objektumok (Attribute)
  - Primary Service
    - Secondary (Included) Service
    - Characteristic (értékek)
      - Descriptor (működés és értelmezés)
- GATT adatbázis a szerveren
  - Bejegyzések azonosítása handle vagy UUID (16-128bit) alapján
- Egyszerű operációk a kliens részéről
  - Felderítési mechanizmusok (discovery)
  - Bejegyzések írása és olvasása
  - Jelzések beállítása (indication, notification)
- **Csatornajellegű kommunikáció helyett adatbázis interakciók**
- Számos előredefiniált (kvázi) szabványos GATT struktúra (Profil)
  - A Bluetooth SIG publikus specifikációi között ezek is megtalálhatók
  - Egy eszközön akárhány Service, vagy Profil lehet



Generic Access Profile (GAP)

- Szerepek (Link Layer állapotok absztrakciói):
  - Central
    - Felderít
    - Kapcsolódást kezdeményez
    - Connection állapotban Master
  - Peripheral
    - Felderíthető
    - Kapcsolódást fogad
    - Connection állapotban Slave
  - Observer
    - Advertising csatornákat figyeli
  - Broadcaster
    - Advertising csatornákon sugároz
- Különböző folyamatok
  - Felderítések, kapcsolódások, stb.
- Definiált struktúrák
  - Pl. GATT Service

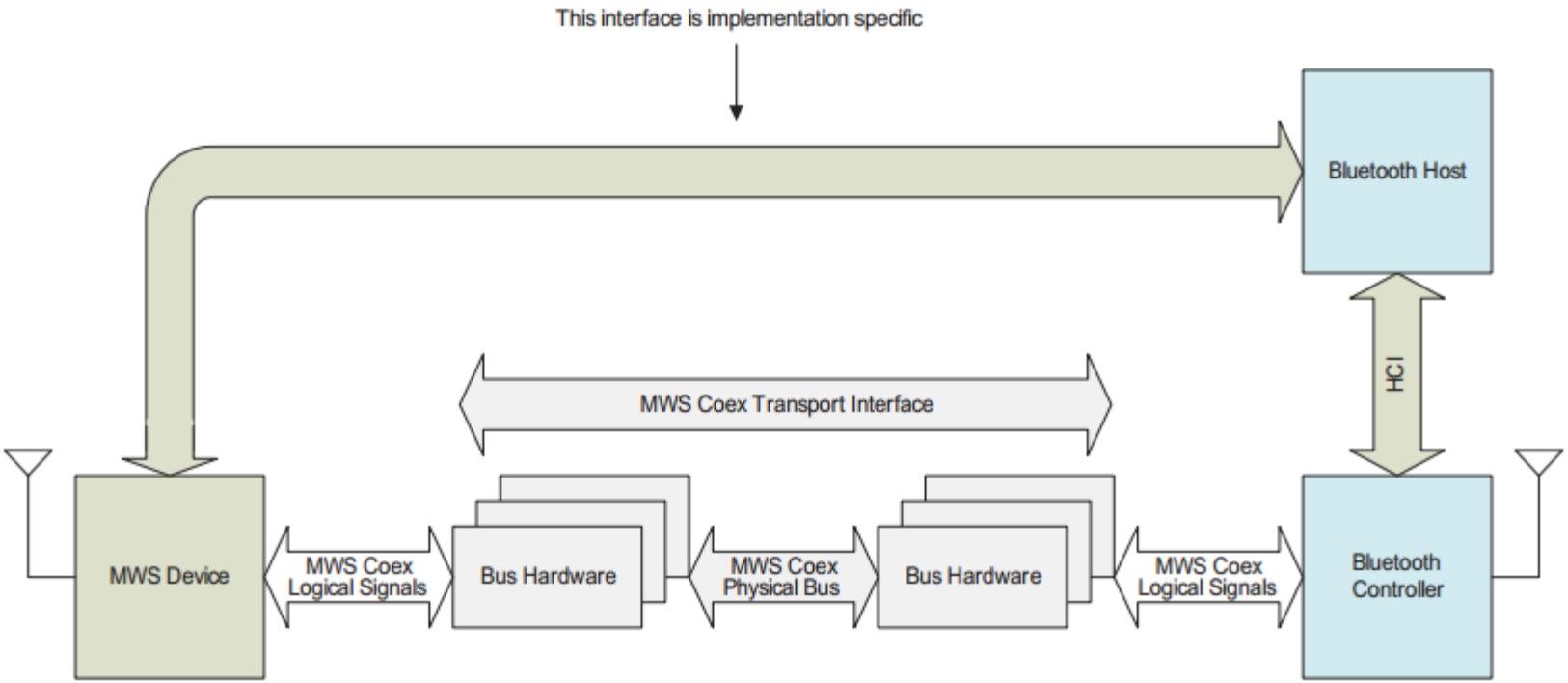


Bluetooth v4.1

- Dual mode eszközök esetén lehet LE-n kapcsolódni
  - v4.0-ban a **hagyományos kapcsolódás** volt ilyen eszközök esetében előírva
- Bluetooth Low Energy Scatternetek bezetése
  - Eredetileg lehetséges volt egyidejűleg több GAP szerepben működni, ha az nem eredményezett tiltott kombinációkat
    - Pl. Egy Slave nem lehetett Master egy másik Piconetben
  - A v4.1-ben ezt a korlátot feloldották, így elérhetővé vált a multihop
    - Párhuzamos GAP szerepek = Párhuzamos LL állapotgépek
      - Ezekből tetszőleges lehet
      - Nem egyszerű megoldani, hogy tényleg működjön
        - » Belső versengés a rádiós interfészért
    - Rengeteg nyitott kérdés, nehéz modellezni
  - Közben elindultak a Broadcast Mesh típusú fejlesztések
    - Multihop az Advertising csatornákon
    - Jellemzően egyszerű megközelítésekkel operálnak
      - Amolyan irányított elárasztás
      - Szebben: Opportunistic Routing, vagy connectionLess IoT

Bluetooth v4.1

- Mobile Wireless Coexistence Signaling
  - Arra az esetre, ha több rádiós technológia használja ugyanazt az erőforrást (pl. rádió)
  - Jelezhető az igény a foglalásra (időrésekben)
    - Prioritásos igények esetén a másik félnek vissza kell lépnie
    - Nem illik állandóan prioritásos igénnyel előállni

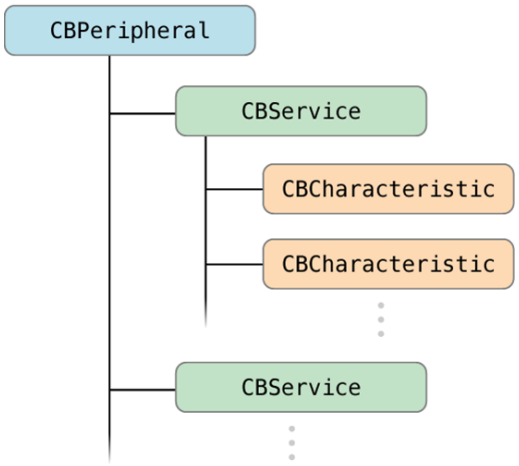


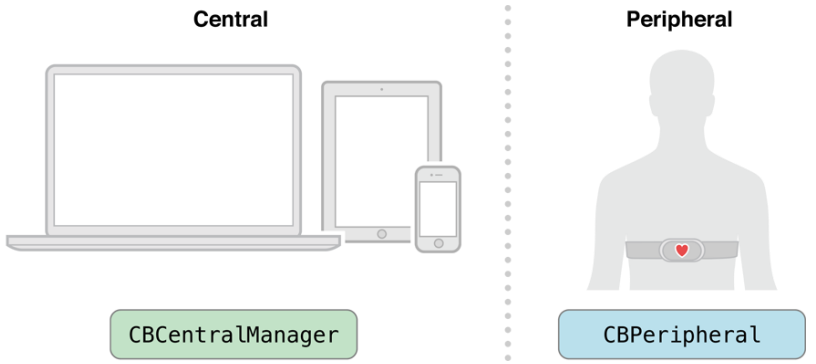
Bluetooth v4.2-v5.0

- Bluetooth v4.2
  - Kiterjesztett csomagméret
    - v4.0-ban fix 47 byte minden PDU (Advertising és Data)
      - Data PDU: 21 oktett hasznos adat
    - v4.2-től 265 byte-os PDU-k is támogatottak (csak Data)
      - Data PDU: 240 oktett hasznos adat
  - Security továbbfejlesztése
- Bluetooth v5.0 (2016 végére, vagy 2017 elejére várható)
  - Amit eddig tudni lehet
    - Konvolúciós kódoló beiktatása (IEEE 802.15.4g javaslat)
    - Max. adási teljesítmény megnövelése 20 dBm-re (100mW)
    - Jelzési sebesség 2 Mbps-ra növelése
      - A csatornák már most is 2 MHz szélesek

BLE a mobil OS-ekben

- iOS - CoreBluetooth Framework
  - iOS 6.0-tól (iPhone 4S)
  - Central (GATT kliens) és Peripheral (GATT szerver)
    - Lokális entitások:
      - CBPeripheralManager, CBCentralManager
        - » CBMutableService
        - » CBMutableCharacteristic
        - » CBDescriptor
    - „Távoli” objektumok:
      - CBPeripheral, CBCentral
        - » CBService
        - » CBCharacteristic
        - » CBDescriptor





BLE a mobil OS-ekben

- Android API Level 18 – Central (GATT kliens és szerver) funkciók
  - Felderítés (startLeScan(…))
  - Kapcsolódás (connectGatt(…))
  - GATT kliens felderítés (getServices())
    - BluetoothGatt{Service, Characteristic, Descriptor}
  - GATT szerver (openGattServer(…))
    - Service regisztráció (addService(…))
- Android API Level 21 – Peripheral funkciók bevezetése
  - Módosított „Central” objektum (BluetoothLeScanner)
  - Peripheral (BluetoothLeAdvertiser)
    - Felderíthetőség (startAdvertising(…))
    - A kapcsolat fogadását az alsóbb rétegek végzik
- Problémák:
  - API 18: Sok hirdetmény (eszköz) kiakasztja a stacket
    - Hákolással üríthetők a tárolók, 3-5s amíg ez végbemegy
  - API 19: Sok hirdetmény után nem hívja a scanCallbacket
    - Az elején is eszközönként csak egyszer
    - Újra kell indítani szkennelést (4/s még működik)

BLE a mobil OS-ekben

- Windows Phone 8-tól
  - Csak előzetesen (kézzel) párosított eszközökkel működik
    - Még a felderítés is…
  - Central (GATT szerver) funkciók
  - Kapcsolódás BluetoothLEDevice példányosítással
  - GATT discovery (device.GattServices(…))
    - GattDeviceService, GattCharacteristic, GattDescriptor

BLE Hardverek

- Legfőbb gyártók:
  - Nordic Semiconductors
  - Texas Instruments
  - Cambridge Silicon Radios (CSR)
- Nagyrészt SoC (System-on-Chip) architektúrát követnek
  - Logika (FW) a Bluetooth IC-n
  - Gyártói SDK-k és BLE Stack implementációk
    - Magas szintű (GAP, GATT, SMP) API-k
    - Jellemzően 3rd party fejlesztőkörnyezetek
      - Windows, Linux
- Egyre inkább „multiprotocol” megoldások
  - Adott egy általános 2,4 GHz-es rádió
    - Ezt különböző módszerekkel lehet vezérelni
  - BLE, ANT, Gazell, stb.

BLE Hardverek

- nRF51(4,8)22 sorozat
  - Általános célú 2,4GHz (GFSK) rádió (API-ból elérhető)
  - ARM Cortex-M0 MCU (128-256K Flash, 16-32K RAM)
- nRF52832 sorozat
  - Általános célú 2,4GHz (GFSK) rádió (API-ból elérhető)
  - ARM Cortex-M4F MCU (512K, 64K RAM)
- SoftDevice BLE stack (v4.1 verzióval konform)
  - Tetszőleges, akár párhuzamos GAP szerep megvalósítható (időosztásban)
- Fejlesztés
  - nRF5 SDK + IoT SDK
  - Külön user és stack space
    - Egymástól kvázi függetlenek
  - Környezetek
    - Linux, Keil uVision (Windows)

BLE Hardverek

- CC2541 sorozat
  - Intel 8051 MCU (128-256K, 8K RAM)
- TI BLE stack
  - GAP szerepek egyenként támogatottak
  - Esetleg Central+Observer és Peripheral+Broadcaster
  - Utolsó update (v1.4.0): 2013. nov. 12.
- Fejlesztés
  - Azonos user és stack space
    - Minden ugyanabban a főciklusban történik
    - A magasabb rétegek megakaszthatják az alsóbbakat
  - IAR Workbench for Intel 8051 (Windows)
    - A BLE stack object kód csak ezzel fordítható