Bluetooth (I)

- Bluetooth è uno Standard Aperto per telecomunicazioni wireless (trasferimento di dati e voce) a corto raggio.
  - [Standard Aperto (Open Standard) vuol dire utilizzabile da chiunque liberamente. Le specifiche sono pubbliche]
- Sviluppato nel 1994 (il nome deriva da Harald Blatant "Bluetooth", Re di danimarca, 940-981 A.D.)
- La trasformazione di bluetooth in standard avviene a opera del Bluetooth Special Interest Group (SIG), fondato nel 1998 e costituito da Ericcson, IBM, Nokia, Intel, Toshiba. Ora più comprende di 1900 società.
- Lo standard Bluetooth serve a realizzare le cosidette Personal Area Network (PAN), cioè piccole reti dell'estensione tipica di qualche metro.

Bluetooth (II)

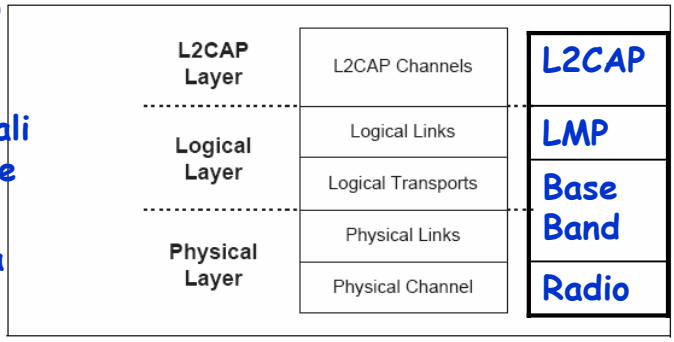
- Lo standard è pensato per essere a basso costo (< 10$ per transceiver). *Nelle intenzioni, un collegamento radio Bluetooth non dovrebbe costare più di un equivalente collegamento con cavo (per es. USB).*
- Banda ISM 2.45 GHz (2400-2483.5 MHz),
- Modulazione Frequency Hopping – Spread Spectrum (FHSS) per ridurre l'effetto di interferenze e fading (cammini multipli).
- Sono disponibili 79 canali FHSS.
- In ogni canale, per minimizzare la complessità del radiotrasmettitore si usa una modulazione binaria FM a 1Msimbolo/s = 1Mbit/s (lordo).
- Da standard, la distanza massima di comunicazione è 10 m (100 m con un trasmettitore potenziato).
- Un ricetrasmettitore bluetooth è anche detto "dispositivo" bluetooth.

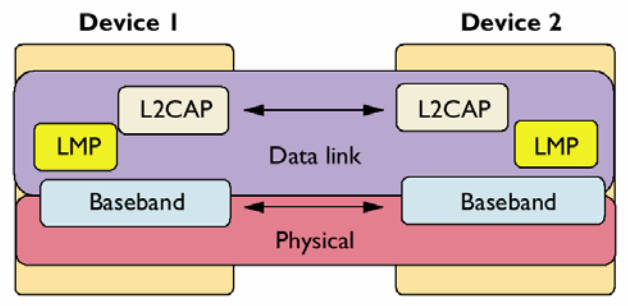
Bluetooth – Strati (I)

- Un canale radio fisico è occupato da più dispositivi sincronizzati su una stessa sequenza di frequency hopping (una "piconet"). Un dispositivo, detto "master", è responsabile della sincronizzazione. Gli altri sono "slave".
- Una rete di Bluetooth è organizzata in strati (layer).
- Abbiamo una serie di canali (channels) e collegamenti (link), e i relativi protocolli:
  - lo strato fisico, composto dal canale fisico (physical channel) e dal collegamento fisico (physical link),
  - lo strato logico, composto dal trasporto logico (logical transport) e da collegamento logico (logical link),
  - lo strato "L2CAP".

Bluetooth – Strati (II)

- Lo strato fisico e buona parte dello strato logico sono descritti dalle specifiche della "banda base bluetooth" (bluetooth baseband). Tali livelli non corrispondono esattamente agli strati del modello ISO-OSI.
- La bluetooth baseband è intermedia tra il livello fisico e il livello collegamento dati (data link) del modello ISO-OSI.
- Il Canale fisico (Radio) corrisponde allo strato fisico del modello ISO-OSI
- La parte più alta dello strato logico è descritta dal Link Manager Protocol (LMP), che è parte dello strato di collegamento (di cui fa parte anche il livello L2CAP).





Specifiche Radio – FHSS (I)

- Per ridurre gli effetti delle interferenze in banda ISM (non regolata), si usa una tecnica di Spread Spectrum, che consente di utilizzare al meglio la banda disponibile:
  83.5 MHz (2.4 GHz - 2.483.5 GHz).

- In particolare, si implementa una tecnica di "Frequency Hopping", cioè di variazione nel tempo della portante secondo una particolare sequenza di salto (hopping) pseudocasuale specifica per ciascuna piconet (FHSS).

- Il Frequency hopping è una tecnica di "collision avoidance" (minimizzazione delle collisioni).
  - Variando la frequenza di trasmissione su tutta la banda ISM si puo' evitare con alta probabilità l'interferenza di altri sistemi di comunicazione a banda stretta fissa o in frequency hopping.

Specifiche Radio – FHSS (II)

- Le frequenze di trasmissione possibili sono:
  - 79, f = 2402 + k MHz (k=0,...,78).
  - banda di sicurezza inferiore di 2 MHz,
  - banda di sicurezza superiore di 3.5 MHz.
- Il tempo è suddiviso in intervalli ("slot") di 625 μs.
- Durante uno slot viene trasmesso un "pacchetto". In alcuni casi è possibile trasmettere pacchetti della durata multipla di uno slot.
- La frequenza di trasmissione viene cambiata, secondo una sequenza pseudocasuale, ogni volta che viene trasmesso un pacchetto.
- Nel caso tipico, in cui un pacchetto ha la durata di uno slot, la frequenza di trasmissione viene quindi cambiata ogni 625 μs ("hopping rate" = 1600 hop/s). Altri casi sono possibili.

Specifiche Radio – TX (III)

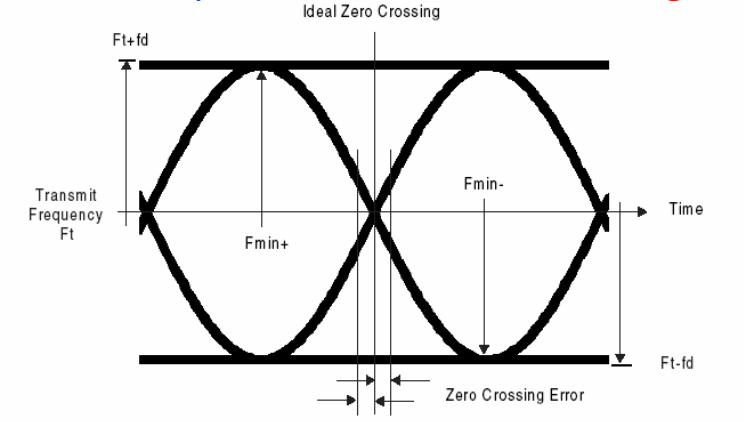
Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

- Il trasmettitore puo' appartenere a una di 3 classi di potenza.
- La classe 3 corrisponde a una potenza massima del trasmettitore di 1 mW (portata massima del sistema di 10 m);
- La classe 1 a una potenza massima di 100 mW (portata massima di 100 m).
- Le antenne (sia trasmettitore, sia ricevitore) sono tipicamente omnidirezionali.

Giuseppe Iannaccone - 2005

Specifiche Radio – Modulazione (IV)

- La modulazone del segnale è GFSK [Gaussian Frequency Shift Keying] con prodotto banda-durata di ciascun bit BT = 0.5,
- data rate di 1 Mbit/s.
- L'indice di modulazione tipico è 0.3 (0.28-0.35).
- Il modulo della deviazione in frequenza fd deve soddisfare
  115 KHz≤fd≤175KHz.
  - Il simbolo "1" corrisponde a una deviazione positiva (fT + fd),
  - il simbolo "0" corrisponde a una deviazione negativa (fT - fd).

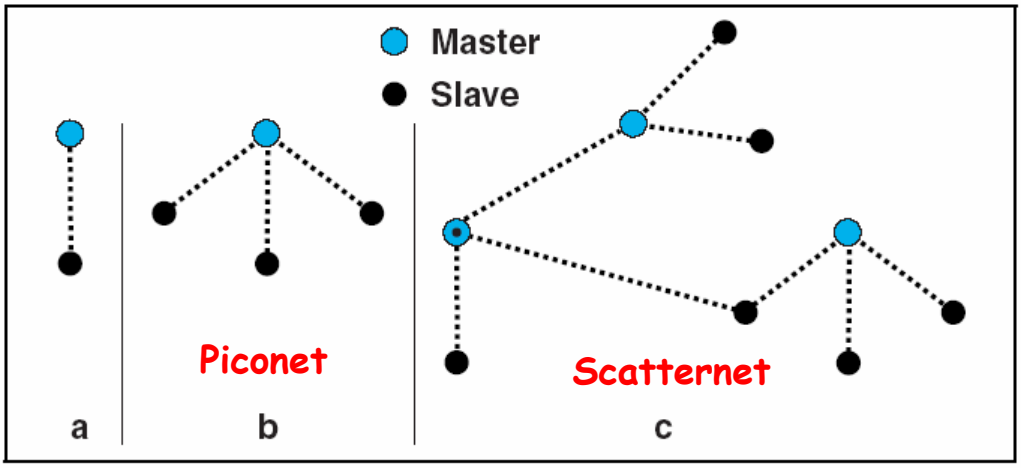


Specifiche Radio – RX (V)

- La modulazione binaria di frequenza permette di realizzare il ricevitore in modo semplice (non deve essere lineare e ci sono solo due simboli), anche se ovviamente limita il bit rate.
- Il ricevitore [unico chip CMOS < 10 $] puo' essere
  - supereterodina con bassa frequenza intermedia (~3MHz)
  - omodina (o "zero IF", cioè conversione diretta da RF a banda video).
- In tutti e due i casi la sensibilità del ricevitore non è particolarmente spinta (nel primo caso la bassa frequenza intermedia impedisce di eliminare la banda immagine, nel secondo caso, l'amplificazione a RF non è particolarmente alta, per cui il rapporto S/N viene deteriorato).
- Lo standard prevede una sensibilità del ricevitore di -70 dBm, per una BER (bit error rate) grezza (cioè escludendo meccanismi di correzione dell'errore) dello 0.1% (es. WiFi – 90 dBm)

Bandabase Bluetooth (Bluetooth baseband)

- La rete elementare bluetooth si chiama "piconet". E' costituita da 2 a 8 radiotrasmettitori.
- Un dispositivo ha il ruolo di "master", gli altri sono "slave".
- Il collegamento fisico puo' essere realizzato solo tra il master e uno slave. Non è possibile avere un collegamento fisico tra due slave.

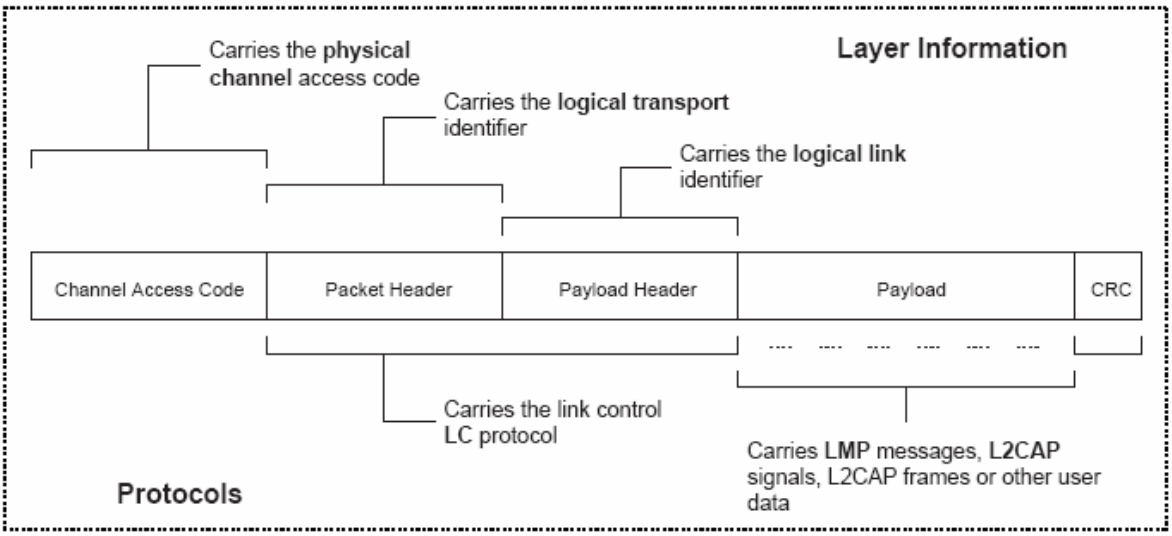


Baseband (II)

- Architettura simmetrica (ciascun dispositivo puo' essere master o slave). Il master è il primo che entra nella piconet
- Un dispositivo puo' inoltre appartenere a piu' di una piconet (come slave o come master), ma puo' essere master solo di una, e in tal caso si chiama "bridge", e permette di unire piu' piconet in una "scatternet".
- Un bridge fa parte di piu' piconet a suddivisione di tempo (time-sharing). In questo modo, è in grado di passare informazioni da una piconet all'altra, rendendo la scatternet connessa.
- I vari ricetrasmettitori della stessa piconet usano il canale fisico a suddivisione di tempo.
- Nel caso in cui ad ogni slot viene cambiata la frequenza di trasmissione, il master trasmette negli slot dispari, e lo/gli slave negli slot pari.

Baseband - Pacchetti (I)

- I dati sono trasmessi in pacchetti, ciascuno costituito da:
  - Codice di accesso (access code): 72 bit
  - Intestazione del pacchetto (packet header): 54 bit
  - Carico pagante (payload): da 0 a 2475 bit
    suddiviso nel payload header, payload vero e proprio, CRC



Baseband - Pacchetti (II)

- Sono possibili diversi **access code**, derivati dal codice identificativo (ID) bluetooth del master o dello slave
  - (ogni dispositivo bluetooth ha un codice identificativo di 48 bit, di cui 24 identificano il costruttore, e 24 un numero seriale assegnato dal costruttore).
- Il pacchetto è accettato da un dispositivo nella scatternet solo se l'access code contiene l'ID del master.

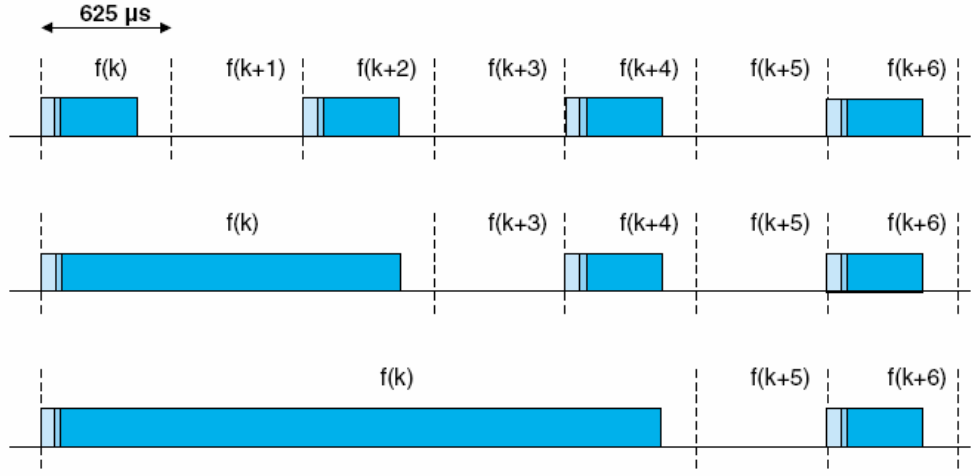
Baseband - Pacchetti (III)

- Il Packet header contiene informazioni sul pacchetto:
  - 3 bit: indirizzo dello slave sulla piconet.
  - 1 bit: positive o negative ack (ACK/NACK)
  - 1 bit: flow flag (flow = 0 STOP nei pacchetti ACL)
  - 1 bit: sequence number (non ci interessa)
  - 4 bit: distingue tra i 16 tipi possibili di Payload:
    - NULL (senza payload), ID (solo codice di accesso), POLL costringe gli slave a risponder, FHS frequency hopping syncronization, + 12 altri tipi di pacchetti sincroni o asincroni (tipo 1: 1 slot; tipo 2: 3 slot; tipo 3: 5 slot, etc…)
  - 8 bit CRC dell'header

  = 18 + altri 36 di ridondanza [FEC 1/3]
- FEC sta per "forward error correction". In FEC 1/3 ogni bit viene trasmesso tre volte consecutivamente. Al ricevitore ogni terna di bit viene interpretata a maggioranza. In questo modo si riesce a correggere un errore singolo per ogni terna di bit.

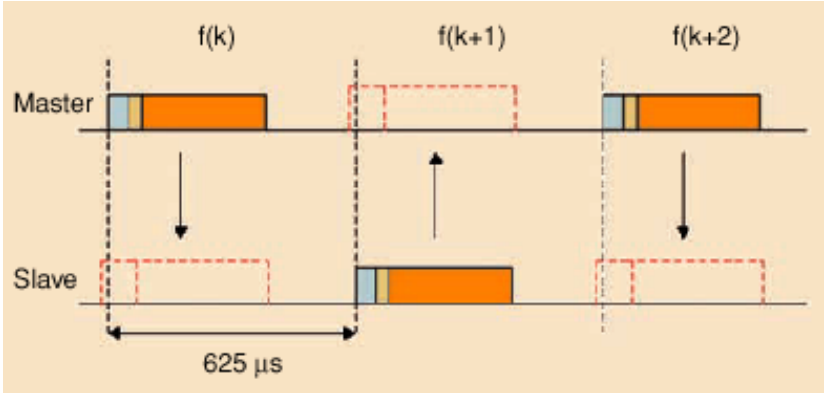
Baseband - Pacchetti (IV)

- Il payload ha un numero di bit variabile in funzione della durata del pacchetto.
- Il pacchetto puo' durare 1, 3, o 5 slot.
- In azzurro sono indicati i pacchetti trasmessi dal master. Gli slave possono trasmettere negli slot rappresentati in figura come vuoti.



Baseband - Pacchetti (V)

- La frequenza di trasmissione viene variata solo alla fine della trasmissione di un pacchetto intero.
- Se il pacchetto dura 3 (5) slot, alla fine del pacchetto si salta direttamente alla frequenza prevista dopo 3 (5) slot, per non perdere la sincronia con la sequenza di hopping.
- Le collisioni sono evitate perché il master decide quale slave deve rispondere, e lo indica nel packet header.



Baseband - Piconet

- Il master ha anche il compito di suddividere la banda disponibile tra i diversi slave.
- Ogni volta che viene modificata la frequenza vanno persi circa 255 μs dello slot, necessari per la variazione di frequenza
  - Se il pacchetto è di uno slot, solo circa 370 μs, sono usati per la trasmissione, corrispondenti a 370 bit.
  - Togliendo i 72 per l'access code e 54 per il packet header, abbiamo circa 244 bit, cioè circa 30 byte.
- Bluetooth consente simultaneamente trasmissione voce (comunicazioni bidirezionali) e trasmissione dati.
- Ci sono quindi diversi collegamenti possibili in bandabase (BASEBAND LINK)
  - Link Sincroni (SCO Synchrounous Connection Oriented)
  - Link Asincroni (ACL Asynchronous ConnectionLess)

Baseband – Link SCO (I)

- I link SCO sono usati per trasmissione voce.
- Sono connessioni simmetriche punto-punto che riservano i time-slot per garantire la trasmissione in tempo reale.
- Il dispositivo slave ha sempre il permesso di rispondere nel time-slot immediatamente successivo a una trasmissione SCO del master.
- Un master puo' supportare fino a 3 link SCO con uno o più slave.
- Uno slave puo' supportare al più 2 link a MASTER differenti.
- I Pacchetti SCO non sono mai ritrasmessi. Se non vanno a buon fine vanno persi.

Baseband – Link SCO (II)

Type	Payload Header (bytes)	Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)
HV1	na	10	1/3	no	64.0
HV2	na	20	2/3	no	64.0
HV3	na	30	no	no	64.0
DV[1]	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D
EV3	na	1-30	No	Yes	96
EV4	na	1-120	2/3	Yes	192
EV5	na	1-180	No	Yes	288

Baseband – Link SCO (III)

- Vediamo le esigenze di un collegamento voce bidirezionale.
- La qualità della comunicazione deve essere ISDN,
- cioè un segnale audio di tipo telefonico campionato a 8 KHz, con 8 bit per campione (256 livelli), per una banda totale di 64 Kbps.
- Per effettuare la comunicazione voce in tempo reale devono essere trasmessi 8 Kbyte al secondo, cioè 10 byte ogni 1.25 ms.
- Poiché nel caso migliore, un pacchetto di uno slot ha 30 byte di carico utile (modalità HV3), è sufficiente uno slot ogni 3.75 ms, cioè uno ogni 6 slot trasmessi.
- Per questo motivo, considerando la comunicazione bidirezionale, 3 comunicazioni voci simultanee saturano completamente il canale radio (ciascuna comunicazione bidirezionale occupa 2 slot ogni 6).

Baseband – Link SCO (IV)

- La modalità HV3 puo' essere impiegata se il canale è in buone condizioni, cioè se senza fare correzione degli errori si ha una comunicazione accettabile. Altrimenti è necessario usare FEC
- La modalità HV2 usa FEC 2/3 [Forward error correction con 2/3 di carico utile]
  - In ogni pacchetto abbiamo 20 byte di carico utile e 10 byte di ridondanza (codice Hamming abbreviato – non vediamo in dettaglio).
  - In questo caso per mantenere il funzionamento in tempo reale con collegamenti di 64 Kbit/s abbiamo bisogno di uno slot ogni 4, quindi il sistema puo' garantire al più due collegamenti voce bidirezionali.
- In condizioni ancora peggiori si usa la modalità HV1, con FEC 1/3 (ripetizione tripla di ogni bit). In questo caso abbiamo un carico utile di 10 byte + 20 byte di ridondanza e quindi un collegamento voce ha bisogno di uno slot ogni 2 (1.25 ms), e quindi è sostenibile un solo collegamento voce.

Baseband – Link ACL

- I link ACL (Asynchronous ConnectionLess) sono usati per trasmissioni dati.
- La trasmissione su questi link è stabilita su una base per-slot (negli slot non riservati ai link SCO).
- I link ACL supportano anche trasferimenti multicast
- Dopo una trasmissione ACL da un MASTER, solo i dispositivi slave indirizzati possono rispondere nel time slot successivo.
- Se non è stato indirizzato nessun dispositivo il messaggio è considerato "broadcast", cioè indirizzato a tutti.
- Tutti i tipi di link ACL includono la possibilità di ritrasmettere i pacchetti.
- La comunicazione dati puo' essere
  - simmetrica
  - asimmetrica.

Baseband – tipi di link ACL

Type	Payload Header (bytes)	Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)	Asymmetric Max. Rate (kb/s)	
						Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6
AUX1	1	0-29	no	no	185.6	185.6	185.6

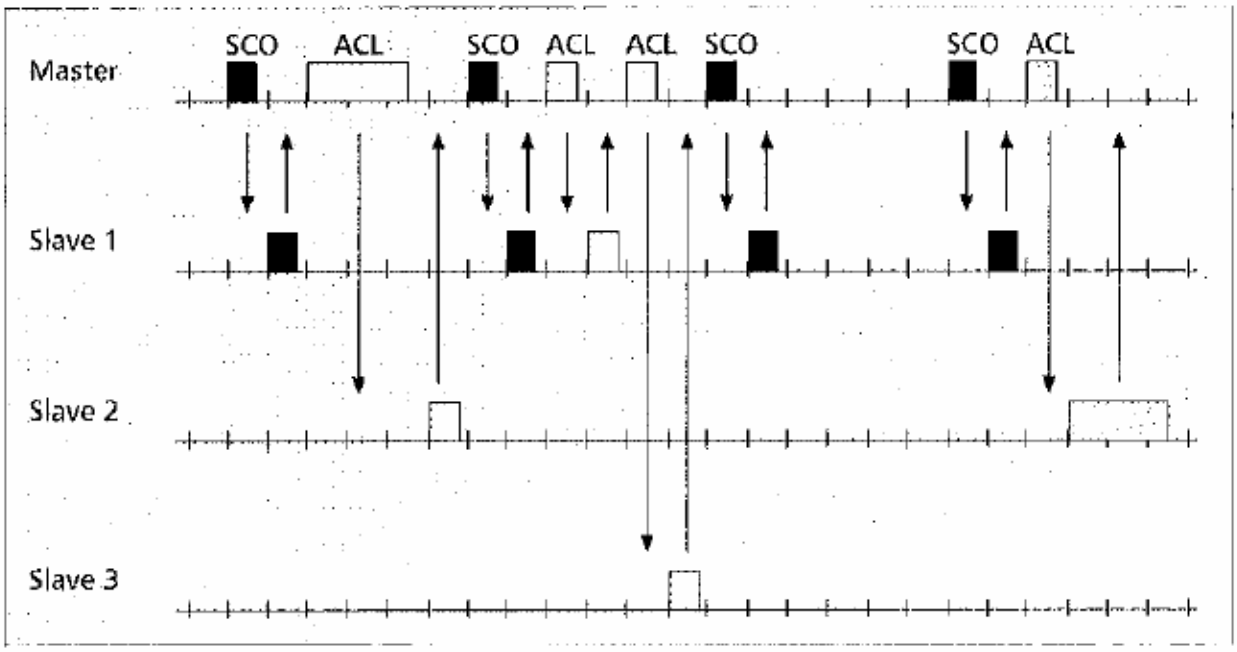
Baseband – Link ACL - simmetrico

- Un pacchetto ha la durata di uno slot.
- Nel caso DH1 dei 30 byte del payload abbiamo
  - Intestazione del payload (1 byte)
  - Carico utile (27 byte)
  - CRC (2 byte)
- Abbiamo quindi una trasmissione di 27 byte netti ogni 2 slot (1.25 ms): 27byte/1.25 ms = 172.8 Kbps
- Nel caso DM1 (tipicamente usato in peggiori condizioni del canale) usiamo una FEC 1/3:
  - Intestazione del payload (1 byte)
  - Carico utile (17 byte)
  - CRC (2 byte)
  - FEC 1/3 (10 byte)
- 17byte/1.25 ms = 108.8 Kbps

Baseband – Link ACL - asimmetrico

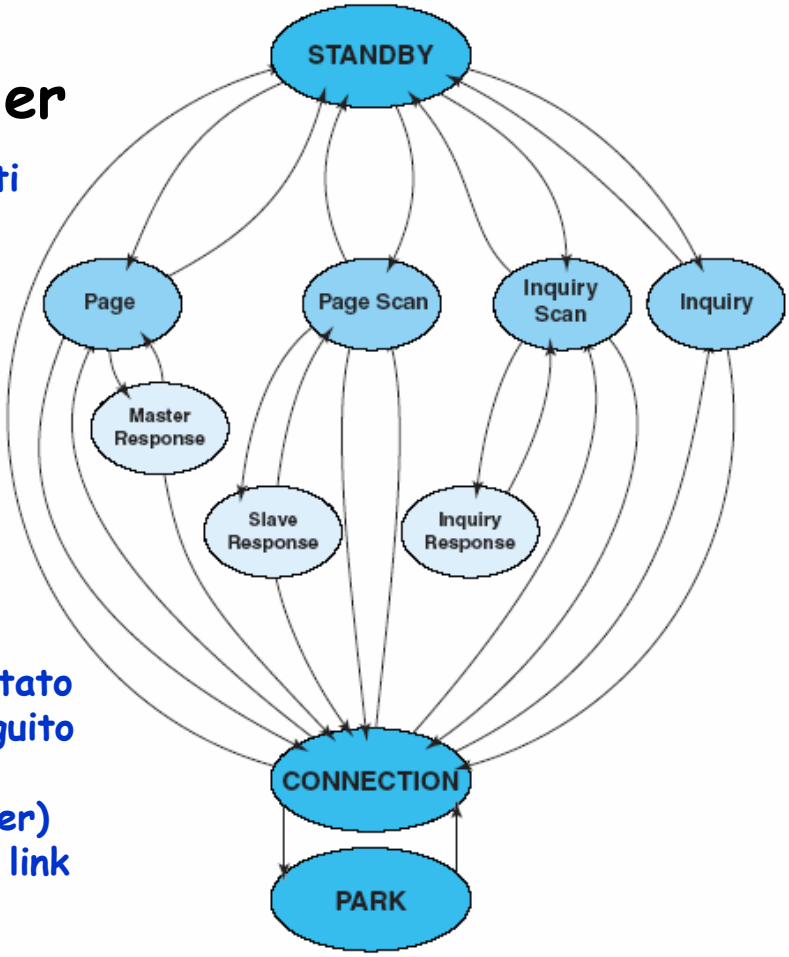
- I pacchetti hanno durata diversa nelle due direzioni.
- Per esempio, nella modalità DH5, vengono alternativamente trasmessi un pacchetto da 5 slot e uno da 1.
- Il pacchetto da 5 slot ha un payload della durata di 4 slot interi in più rispetto al pacchetto da 1 slot.
- In 4 slot interi (2.5 ms) stanno 2500 bit = 312.5 byte in più, quindi il payload ha complessivamente 244+2500 = 2744 bit (343 byte): Intestazione del payload (2 byte), Carico utile (339 byte), CRC (2 byte)
- Il pacchetto viene trasmesso ogni 6 slot. Il data rate nella direzione più veloce è quindi: 339*8 bit/3.75 ms = 723.2 Kbps. Questo è il massimo datarate.
- Nell'altra direzione viene trasmesso un pacchetto da uno slot (27 byte utili) ogni 6 slot, cioè: 27*8 bit/3.75 ms = 57.6 Kbps.

- Il sistema puo' tenere aperto contemporaneamente canali voce e dati, a suddivisione di tempo. Un esempio della sequenza, con un canale voce (SCO) e uno o più dati (ACL), è mostrato nella figura in basso.



Link Controller

- E' la Macchina a Stati che controlla i collegamenti
- Ogni dispositivo nella piconet ha 3 stati principali possibili:
  - STAND BY
  - CONNECTION
  - PARK
- + 7 stati intermedi
- Il passaggio da uno stato all'altro avviene a seguito di comando dal livello superiore (link manager) o comandi interni del link controller.



Baseband - Link Controller (I)

- Stato STAND-BY:
  - E' lo stato di default del dispositivo, ed è un "low power mode". Solo il clock interno funziona in modo continuativo.
  - Ogni 1.28-3.84 secondi il dispositivo si mette in ascolto, cioè passa nello stato PAGE SCAN o INQUIRY SCAN tipicamente per 10 ms (cioè 16 slot).
  - Puo' inoltre uscire dallo stato STANDBY per cominciare la ricerca di altri dispositivi, andando nello stato PAGE o INQUIRY.

Baseband - Link Controller (II)

- **Stato PAGE SCAN:**
  - il dispositivo si pone in ascolto (RX on) per una finestra di 10 ms (16 slot), per rispondere eventualmente a un altro dispositivo che sta cercando di formare una nuova connessione.
  - La frequenza di funzionamento è costante durante ciascuna finestra, e tra una finestra e l'altra viene cambiata seguendo la sequenza di page hopping ("page hopping sequence"), che dipende dal proprio ID bluetooth.
  - Passato il tempo di ascolto il dispositivo torna nello stato di provenienza, che puo' essere STAND BY o CONNECTION.
  - Se durante la finestra temporale riceve il messaggio "page" inviato da un altro dispositivo, va nello stato SLAVE RESPONSE e comincia la procedura di attivazione della connessione

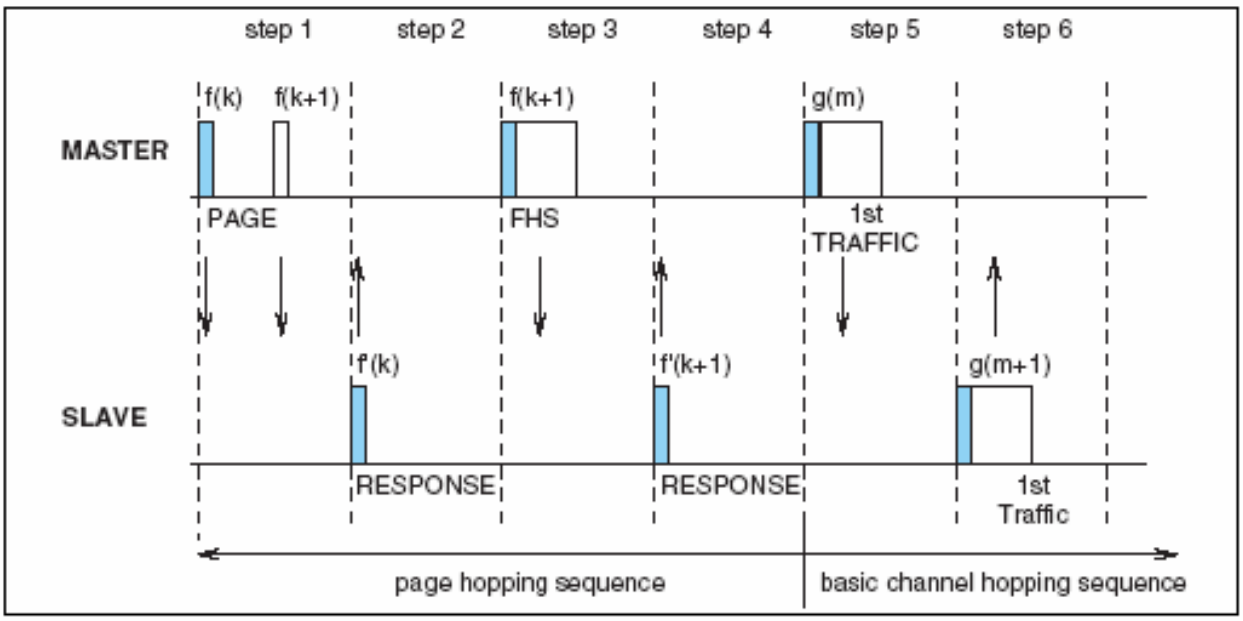
Baseband - Link Controller (III)

- **Stato PAGE:**
  - E' usato da un dispositivo per attivare una nuova connessione con uno slave nello stato PAGE SCAN.
  - Il dispositivo diventerà il master di una nuova piconet, se si tratta della prima connessione, o è già il master della piconet esistente (lo chiamiamo "master")
  - Il master deve conoscere l'ID (il numero seriale bluetooth) dello slave con il quale vuole stabilire la connessione.
  - L'ID puo' essere conosciuto per la storia precedente (noto da precedenti collegamenti, o dal programma di applicazione), o puo' essere stato determinato attraverso una precedente fase di "inquiry".

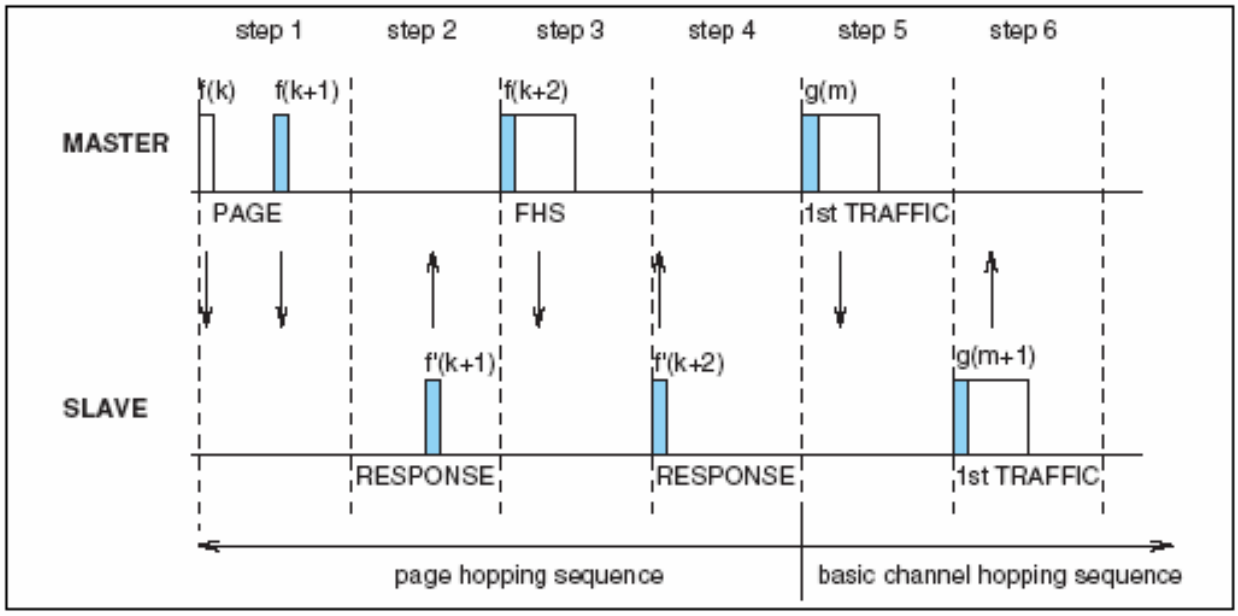
Baseband - Link Controller (IV)

- **Stato PAGE** (..continua):
  - Negli slot dispari il master trasmette due messaggi "page",
    - contenenti solo l'access code dello slave (68 ms)
    - variando la frequenza di trasmissione ogni metà slot, secondo la sequenza di page hopping.
    - Se lo slave desiderato è nello stato PAGE SCAN e sta ascoltando alla frequenza di trasmissione, questi risponde e si puo' stabilire la connessione.
- La sequenza di page hopping è una sequenza pseudocasuale che comprende solo 32 delle frequenze possibili.
- Nella finestra temporale di ascolto del PAGE SCAN ci sono 16 slot, cioè 8 slot dispari, durante i quali il master trasmette il comando "page" a 16 frequenze diverse, delle 32 possibili. La probabilità di stabilire il contatto con il nuovo slave durante una finestra temporale è del 50%.

- Sequenza dei messaggi quando lo slave riceve il comando page nella prima metà dello slot.
- Nello step 1 il master è nello stato PAGE, lo slave nello stato PAGE SCAN. Nello step 2 lo slave è nello stato SLAVE RESPONSE, il master nello stato PAGE. Nello step 3 il master è nello stato MASTER RESPONSE.



- Sequenza dei messaggi quando lo slave riceve il comando page nella seconda metà dello slot.



Baseband – Link Controller (V)

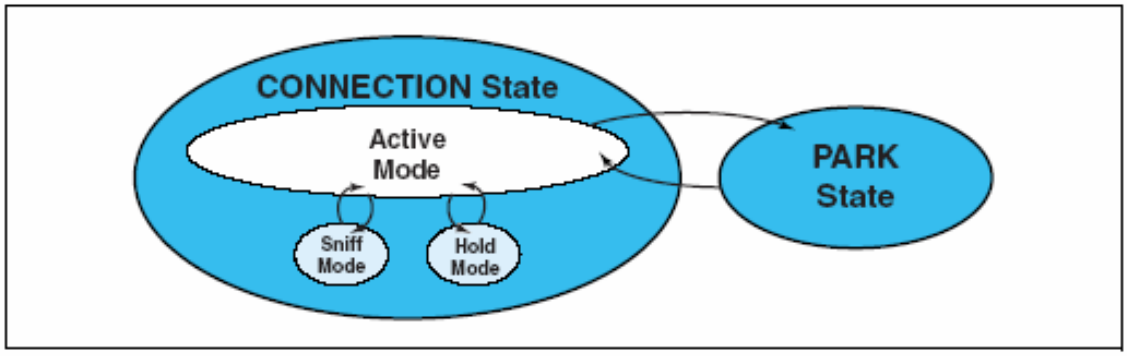
- Stati SLAVE RESPONSE e MASTER RESPONSE:
  - Nello step 2 lo slave risponde (SLAVE RESPONSE) inviando un pacchetto di acknowledgment con solo l'access code (cioè il proprio ID), esattamente 625 μs dopo il page a cui risponde
  - Quando il master riceve tale pacchetto va nello stato MASTER RESPONSE e invia il comando FHS (frequency hopping sequence) che fornisce le informazioni allo slave per sincronizzarsi sulla sequenza di hopping principale
    - (in particolare, contiene l'ID del master, informazioni sulla fase del clock, e indica da quale punto della sequenza di hopping si parte).
  - Lo slave manda un'altra risposta per confermare la ricezione di FHS. Nello step 5 master e slave sono entrambi nello stato CONNECTION, e cominciano a trasmettere seguendo la sequenza di hopping normale. Il master trasmette il suo primo pacchetto utile nello step 5, lo slave nello step 6, e così via.

Baseband – Link Controller (VI)

- **Stato INQUIRY:**
  - E' lo stato in cui un dispositivo verifica se ci sono altri dispositivi bluetooth nelle vicinanze. Trasmette due volte per slot il messaggio "inquiry", contenente solo un codice d'accesso (senza il proprio ID) con la sequenza di page hopping.
  - Negli slot pari, ascolta i dispositivi che rispondono con un "inquiry response" e raccoglie gli ID. Se, successivamente vuole stabilire una connessione con questi dispositivi, si sposta nello stato page.
  - Un dispositivo accede allo stato INQUIRY da STANDBY o da CONNECTION. Dopo un certo tempo, determinato dai livelli superiori, torna nello stato di origine
- **Stato INQUIRY Scan.**
  - E' praticamente identico allo stato page SCAN. Se riceve un messaggio di inquiry, passa nello stato INQUIRY RESPONSE, in cui, dopo 625 μs invia un messaggio di risposta in cui specifica il proprio ID, e informazioni sulla fase del proprio clock

Baseband – Link Controller
Stato Connection

- **Stato CONNECTION:**
  - E' lo stato tipico della piconet, che permette le comunicazioni bidirezionali tra master e slave. Nello stesso stato un dispositivo puo' sospendere temporaneamente la connessione
  - Nello stato Connection, un dispositivo puo' essere in tre modi di funzionamento: ACTIVE MODE, SNIFF MODE, HOLD MODE.

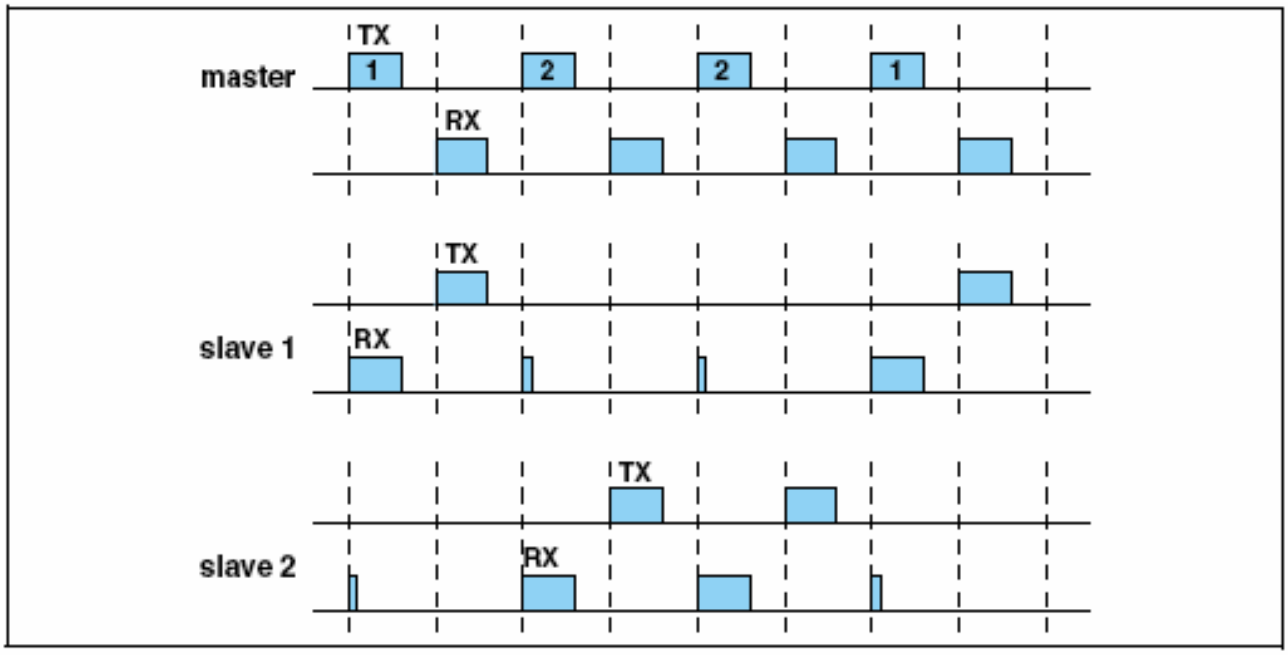


Baseband – Link Controller –Active Mode

- Possono essere nel modo attivo al più il master e sette slave.
- I dispositivi attivi supportano la comunicazione bidirezionale.
- Il master distribuisce la banda tra i vari slave, e consente loro di rispondere.
- Nel caso di comunicazione con più slave, ciascuno slave ascolta il master negli slot dispari (master-to-slave), e smette di ricevere se l'intestazione del pacchetto non contiene il suo numero identificativo nella piconet.
- Solo lo slave effettivamente indirizzato ascolta tutto il pacchetto, e risponde nello slot successivo.
- In questo modo si riesce a ridurre il consumo di potenza.

- Nel modo attivo si puo' cambiare il master della piconet.

Active Mode – esempio di temporizzazione



Stato Connection – modi Sniff e Hold (I)

- I modi SNIFF e HOLD permettono un risparmio di potenza.
- Nel modo SNIFF il duty cycle di attività di un dispositivo slave viene ridotto di una quantità determinata in accordo tra master e slave.
- In pratica il master o lo slave invia il comando "sniff" tramite il link manager, con argomento Nsniff intero.
- Da quel momento, lo slave ascolta un slot dispari (master-to-slave) ogni Nsniff slot dispari.
  - Se viene indirizzato risponde nello slot successivo, altrimenti spegne il ricevitore e lo riaccende dopo Nsniff slot.
  - Il master, a sua volta, sa a quali slot puo' interrogare lo slave in modo sniff.

Stato Active – modi Sniff e Hold (II)

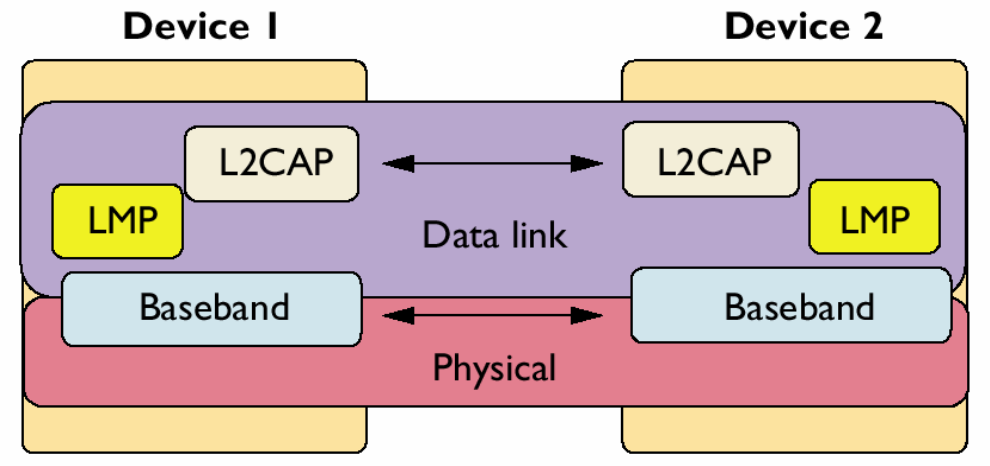
- Il master puo' ordinare a un dispositivo in modo attivo (anche se stesso) di passare al modo HOLD per un tempo prefissato Thold.
- Durante questo tempo, il dispositivo non ascolta più quello che viene trasmesso sui link ACL (continua a mantenere eventuali link SCO), ma continua a seguire la sequenza di hopping.
- Mentre è in HOLD è libero di fare paging, inquiry, o comunicare su un'altra piconet (se fa da bridge).

Baseband – Link Controller - Stato Park

- Stato PARK:
- Nello stato PARK uno slave esce dalla piconet, e mantiene solo la sincronizzazione con la sequenza di hopping.
- Il dispositivo lascia libero l'indirizzo nella piconet (da uno a sette) e prende un indirizzo di parcheggio.
- E' uno stato può consentire di aumentare in modo virtuale i dispositivi di una piconet oltre il numero di massimo di 8.
- Il dispositivo nello stato PARK non ascolta più.
  - Si risveglia a intervalli periodici per ascoltare eventuali messaggi dal master.
  - Se il master vuole risvegliare o inviare un comando a un dispositivo parcheggiato invia un "beacon", cioè un treno di pacchetti identici ripetuti un numero di volte sufficiente a garantire che il dispositivo parcheggiato si svegli almeno una volta e ascolti.

Link Manager (LM) e Link Manager Protocol (LMP)

- La macchina a stati in bandabase è controllata dal LINK MANAGER, che è un FIRMWARE (un software contenuto nella ROM e contenente routine e primitive di basso livello) fornito insieme all'hardware di controllo del link.

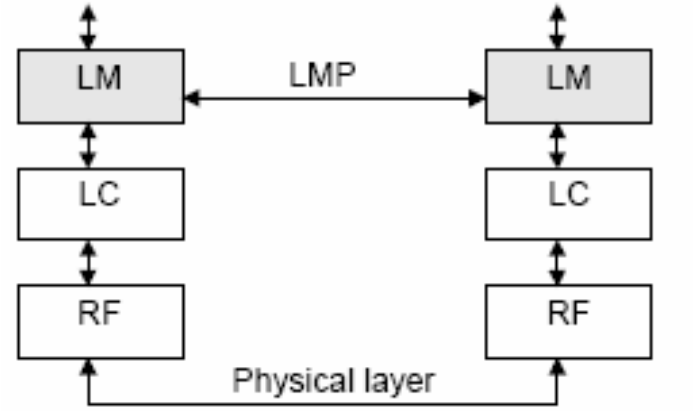


Link Manager

- Il link manager stabilisce la connessione, la controlla, e ne garantisce la sicurezza.
- Ha le seguenti funzioni:
  - Autenticazione della comunicazione sul link e sicurezza
  - Monitoraggio della qualità del servizio (QoS Quality of Service)
  - Controllo della banda base Bluetooth
  - Controllo e gestione del paging
  - Controllo e gestione dello stato degli slave
  - Controllo del cambiamento di master nella piconet.
  - Gestisce i pacchetti multislot e gestisce l'allocazione degli slot tra i vari link.
- Il master ha il compito di dividere il tempo del collegamento tra i vari ACL (facendo polling (interrogandoli) più spesso o usando pacchetti più o meno lunghi).

Link Manager Protocol (I)

- I link manager comunicano tra di loro tramite il Link Management Protocol (LMP), che controlla e negozia tutte gli aspetti della messa in opera e gestione dei collegamenti tra più dispositivi.

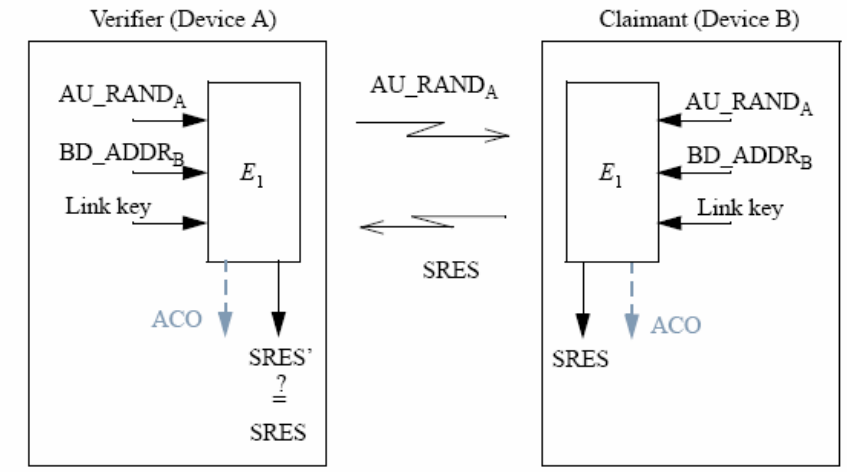


- Il LMP consente la comunicazione ai link manager di due dispositivi connessi da un link ACL.
- Tutti i messaggi e i comandi LMP sono trasmessi come carico utile dei pacchetti ACL, differenziati tramite l'header ACL dai messaggi e comandi del protocollo L2CAP

Link Manager Protocol - Autenticazione

- L'autenticazione avviene con uno schema "challenge-response".
- Il dispositivo che si vuole far autenticare è il richiedente ("claimant"). Il dispositivo che verifica l'autenticità si chiama verificatore ("verifier").
- L'autenticazione ha successo se il verificatore e il richiedente condividono la stessa chiave K, nel nostro caso la "link key", che è stata generata appositamente per il collegamento tra quei due dispositivi e viene verificata tutte le volte che i due si collegano (finché non viene cambiata).
  - Il verificatore (A) genera un numero casuale di 128 bit (AU_RANDA) [la "challenge"] e lo invia al richiedente (B).
  - B usa l'algoritmo E1 con argomenti
    - AU_RANDA,
    - il proprio bluetooth address BD_ADDRB,
    - e la chiave segreta K (128 bit), e ottiene
    - SRES = E1(AU_RANDA, BD_ADDRB, K), di 32 bit.

.. Autenticazione



- B invia SRES ad A
- A verifica se SRES è uguale al valore SRES' generato internamente con la propria chiave K. Se le chiavi sono uguali e il BD_ADDRB è giusto l'autenticazione è completata.

- Se l'autenticazione deve essere mutua, dopo questo passo B puo' fare da verificatore e A da richiedente, e B puo' mandare una challenge AU_RANDB ad A per la verifica.
- Insieme a SRES, E1 genera anche ACO, che viene usata successivamente per la cifratura.

Pairing

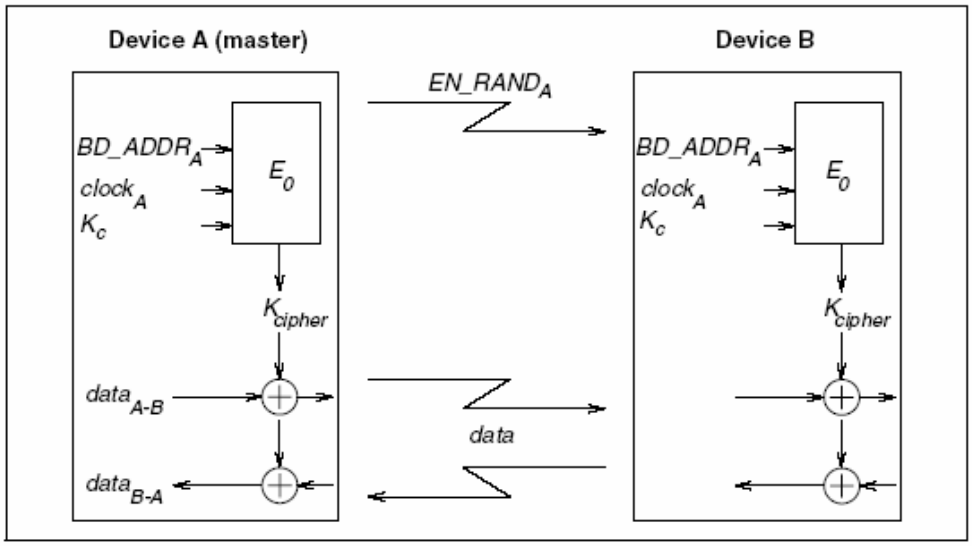
- Il Pairing è la procedura di inizializzazione del link, durante il quale viene generata la chiave di inizializzazione, dalla quale è ottenuta la chiave segreta del link,
- La chiave di inizializzazione si ottiene a partire da
  - un PIN, l'indirizzo bluetooth dei dispositivi, e un numero casuale.
- Il PIN deve essere inserito dall'utente con una procedura che dipende dal particolare dispositivo bluetooth.
- Una volta che la chiave di inizializzazione è generata, la chiave segreta del link viene generata con procedura di autenticazione mutua all'inizio del collegamento, a partire da un numero casuale che il master spedisce allo slave.

Cifratura (I)

- La cifratura puo' essere effettuata dopo che almeno una autenticazione ha avuto luogo.
- La cifratura consiste semplicemente una somma modulo 2 bit a bit tra il pacchetto da spedire in uno slot e una chiave altrettanto lunga (Kcypher).
- Kcypher viene generata con un algoritmo EO che ha come argomenti:
  - BD_ADDRA, una chiave per la cifratura K_C e il valore del contatore (clock) del master (26 bit):
- Kcypher = Kcypher(BD_ADDRA, K_C, clock)
- La chiave per la cifratura K_C viene ottenuta come funzione di un numero casuale EN_RANDA di 128 bit, la "link key", e della stringa *ACO* ottenuta in fase di autenticazione
  - [K_C = K_C(EN_RANDA, link key, *ACO*)]

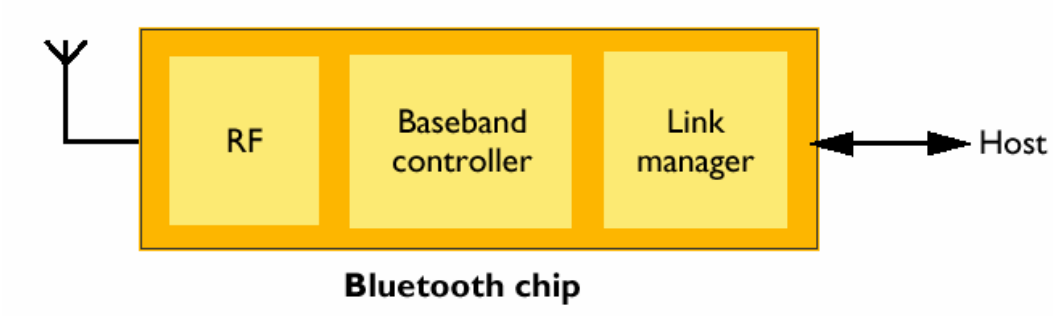
Cifratura (II)

- EN_RANDA viene generato dal master e spedito in chiaro all'inizio dell'operazione di cifratura.

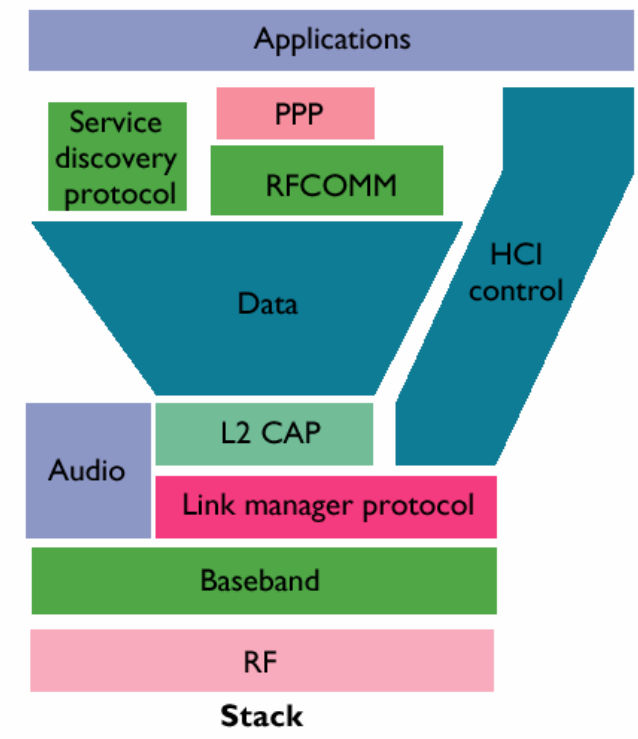


Bluetooth Chip

- Tipicamente la sezione RF, i circuiti di controllo della banda base Bluetooth e i link manager non contenuti in un unico chip bluetooth, che poi è inserito in un sistema "ospite".
- Gli strati inclusi nel chip sono realizzati via hardware o firmware.
- I livelli superiori sono implementati tipicamente via software (tranne l'HCI).



Strati superiori dello standard

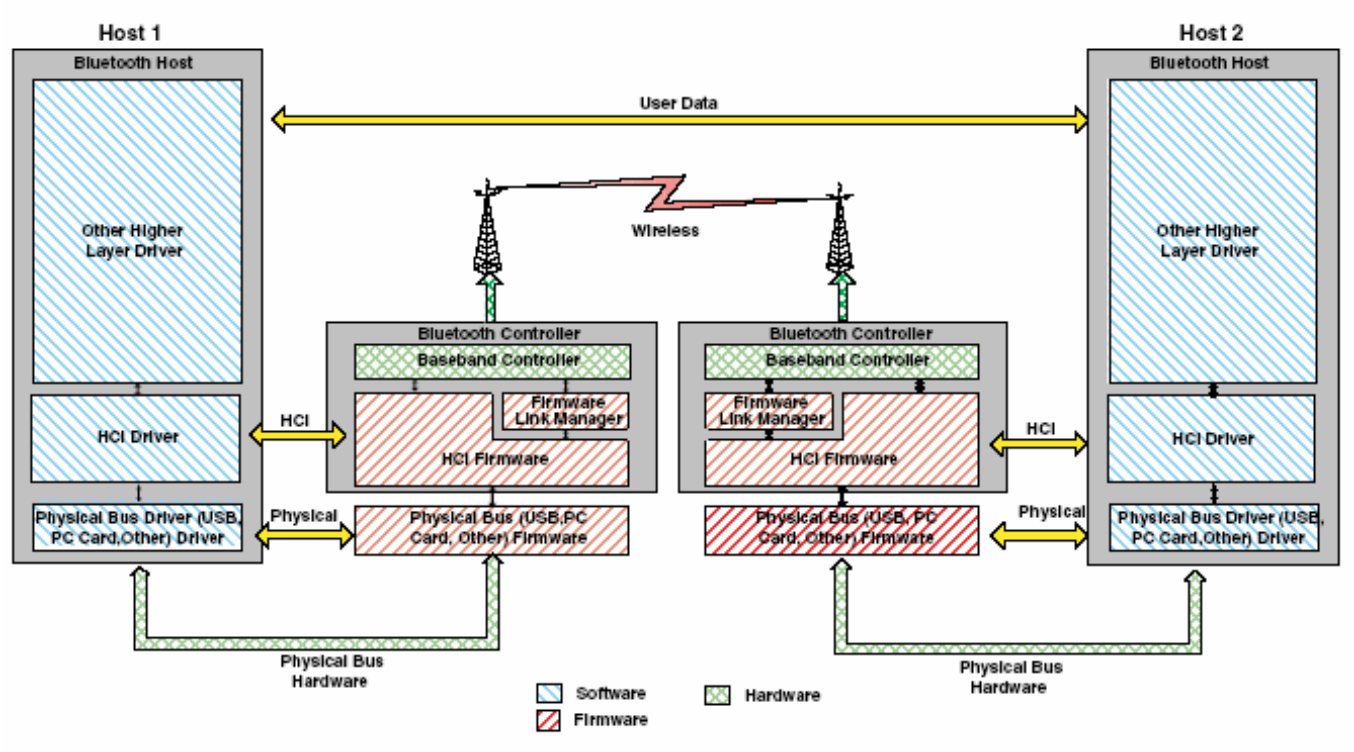


- Nota:
  - l'audio non è gestito da LMP
  - in realtà parte di HCI sta sotto L2CAP
- Dei livelli superiori all'LMP dedichiamo spazio solo a
  - L2CAP (Logical Link Control and Adaptation Protocol), e
  - HCI (Host Control Interface).

HCI – Host Control Interface

- HCI consente l'interfacciamento del chip bluetooth con il sistema ospite attraverso gli standard via cavo più comuni, come USB, RS232, UART.
- E' realizzato tipicamente via firmware, o firmware/software.
- Supponiamo che Host 1 e Host 2 siano forniti di due schede bluetooth, collegate tramite un bus fisico, per esempio USB.
- I due Driver HCI degli ospiti comunicano usando i servizi messi a disposizione dalla HCI.
- I dati vengono scambiati tra ospite e scheda bluetooth in accordo al protocollo del bus fisico, e tra le schede bluetooth come carico utile di un link ACL.

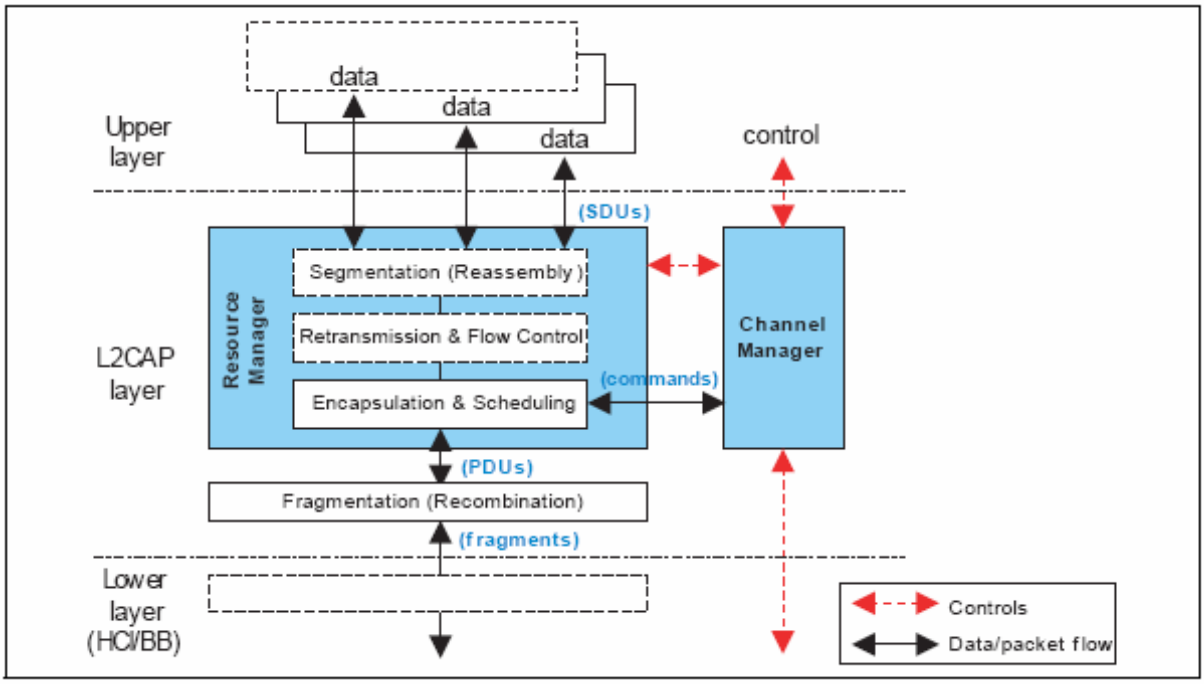
Schema HCI



L2CAP
Logical Link Control and Adaptation Protocol

- L2CAP è uno strato intermedio (del livello data link) che garantisce
  - il multiplexing dei protocolli superiori;
  - l'interoperabilità tra dispositivi bluetooth;
  - gestione del gruppo mappando i protocolli di gruppo superiori sulle reti piconet
    - (per esempio deve mappare sui protocolli inferiori la comunicazione tra due slave della stessa piconet);
  - la segmentazione e riassemblamento dei pacchetti tra livelli;
  - la negoziazione e monitoraggio della qualità del servizio (dei protocolli superiori).

L2CAP



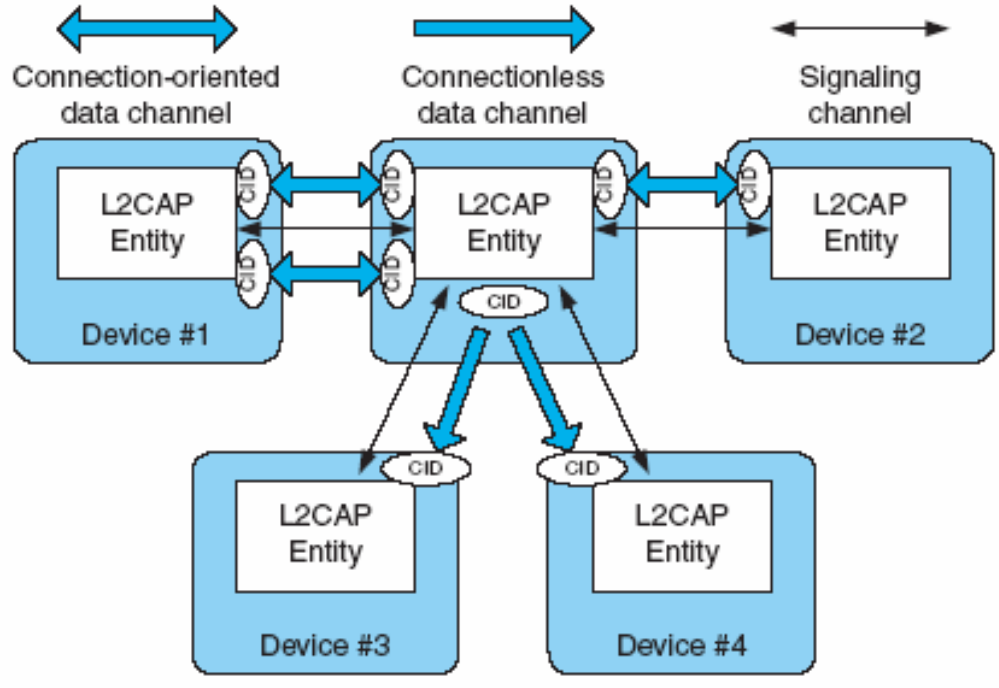
L2CAP (III)

- I messaggi L2CAP costituiscono carico utile dei link ACL, con priorità inferiore ai pacchetti LMP (LMP deve garantire l'integrità del collegamento e ha quindi massima priorità).
- I messaggi e comandi L2CAP vengono spediti su canali L2CAP, che a loro volta usano i link ACL esistenti
  - (nota: un collegamento indica una connessione fisica (basso livello), un canale indica una connessione software (alto livello))
- Abbiamo canali di tre tipi:
  - canali di segnalazione bidirezionali (comandi)
  - canali orientati alla connessione (CO – Connection Oriented) (connessioni bidirezionali punto-punto)
  - conali unidirezionali senza connessione (CL - ConnectionLess) (connessione da punto a multipunto, che permettono a una entità L2CAP di essere collegata a un gruppo di dispositivi remoti).

Canali L2CAP

- Ogni canale L2CAP include due **endpoint** indentificati da un **CID di 16 bit** (CID Channel ID - Identificatore di canale logico).
- Il Canale di segnalazione ha CID = 0001
- Ogni canale CO ha un CID locale allocato dinamicamente ed è legato ad uno SPECIFICO protocollo di livello superiore.
  - Durante la configurazione si negozia la qualità del servizio (QoS) di ogni canale (banda di picco, tipo di trasmissione (best effort, garantita, no traffic)).
- I canali connectionless (CL) sono unidirezionali e sono usati per formare gruppi.
- Un **endpoint CL outgoing** puo' essere logicamente collegato a più **endpoint CL ingoing**, che formano un gruppo logico.
- Ogni entità L2CAP ha un solo endpoint CL ingoing (indirizzo CID = 0002). I canali CL non richiedono connessione o configurazione.

Esempio della rete a livello delle entità L2CAP

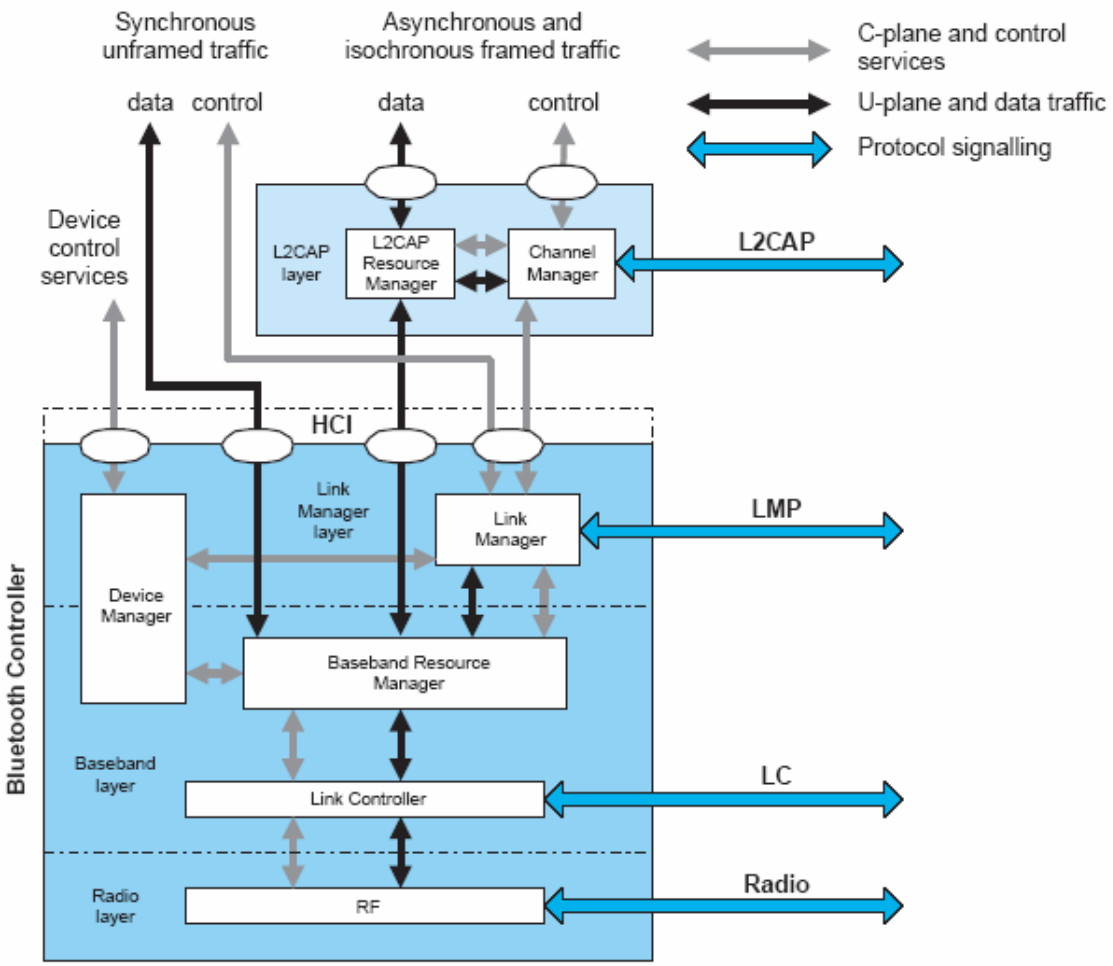


Macchina a stati dell'entità L2CAP

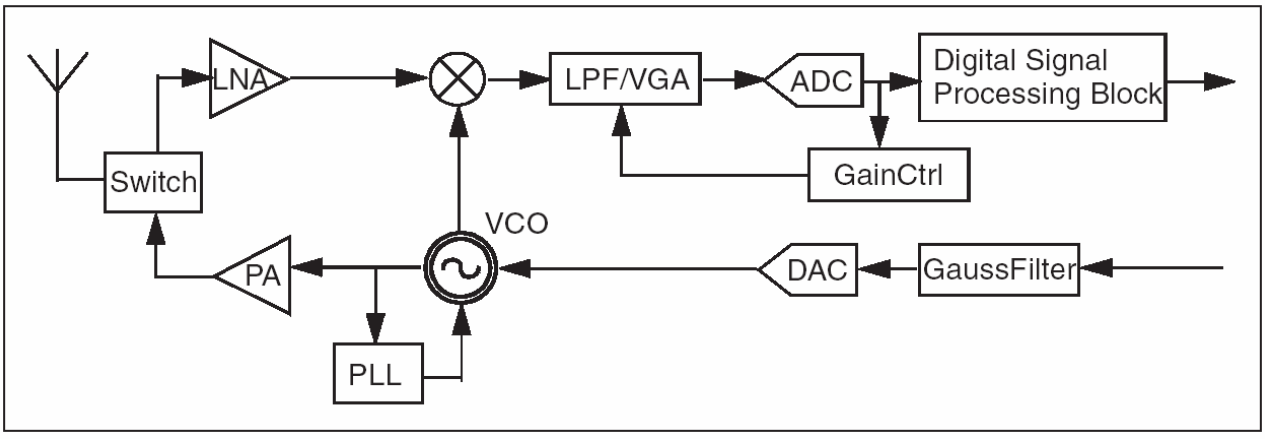
- Un end-point L2CAP puo' essere in più stati:
  - OPEN: è possibile il trasferimento dei dati
  - CLOSED: nessun canale è associato al CID
- La connessione viene aperta se l'entità L2CAP locale richiede la connessione a un dispositivo remoto, o se l'entità L2CAP locale riceve una richiesta di connessione al proprio CID.
- Nel primo caso la richiesta è partita dal protocollo di grado pià elevato.
  - L'entità entra nello stato "W4_L2CAP_Connect_RSP" e aspetta una risposta.
- Nel secondo caso, l'entità passa la richiesta al livello superiore se si mette nello stato "W4_L2CAP_Connect_RSP".
  - Quando arriva la conferma, il dispositivo va nello stato CONFIG. Una volta completata la configurazione, i due dispositivi entrano nello stato OPEN e cominciano a scambiarsi dati.

Macchina a stati dell'entità L2CAP

- La chiusura della connessione comincia quando un'entità manda una disconnection request all'altra .Entra nello stato "W4_L2CAP_DISCONNECT_RSP" e alla risposta va nello stato CLOSED.
- Dimensione dei pacchetti:
- Canali CO:
  - 32bit header (16bit lunghezza + 16 bit CID)
  - payload (0-65535 byte).
- Canali CL:
  - 32 bit header (16 bit lunghezza + 16 CID (CID=0002h)
  - PSM (protocol/service multiplexer) ≥ 16bit, che indica da che protocollo di livello più alto il pacchetto proviene.
  - payload (0-65535 byte)

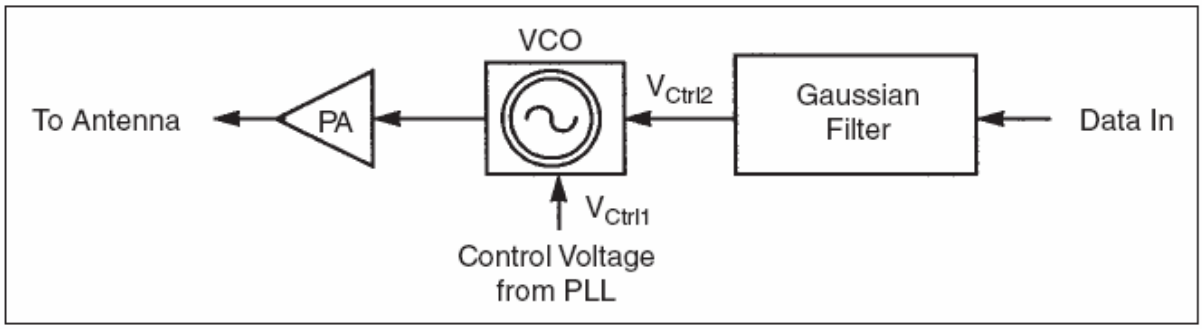


Architettura di un transceiver Bluetooth



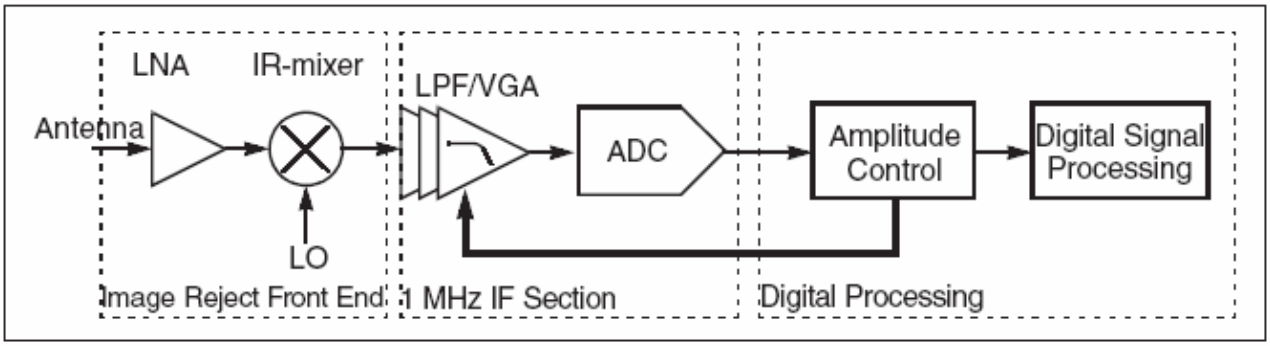
- Sintetizzatore di frequenza con VCO e PLL
- Selezione del canale, demodulazione, e correzione della frequenza sono tutte implementate in modo digitale per consentire facilmente migrazioni verso nodi tecnologici più avanzati e integrazione su unico chip

Trasmettitore



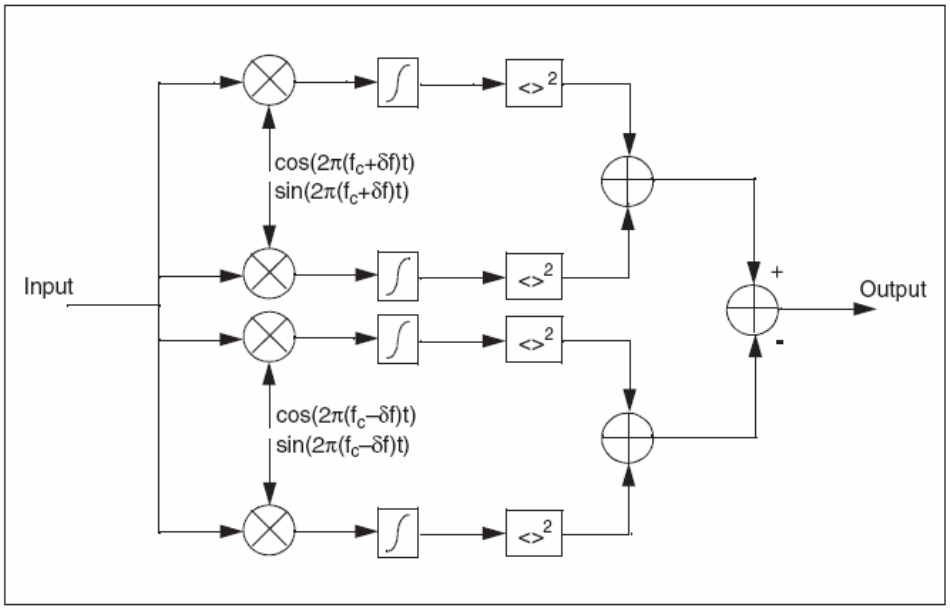
- Il PLL viene usato per accordare la frequenza e poi L'anello di reazione del PLL viene aperto quando si trasmette (FSK)
- Alla fine del pacchetto il PLL si riaggancia, ma c'e' sicuramente stato una deriva. Bluetooth per questo motivo consente una deriva di ±25 KHz per i pacchetti DH1 e di ±50 KHz per DH3 e DH5. Offset iniziale ±75 KHz
- Filtro Gaussiano in Digitale seguito da DAC

Front End del Ricevitore



- Il mixer spesso non è a reiezione dell'immagine
- La frequenza dell'oscillatore locale e' ottenuta dallo stesso VCO usato in trasmissione. Il PLL è aperto anche in ricezione (per evitare spurie provenienti dal PLL). Si ha deriva della frequenza LO
- Bassa IF
- Low Pass Filter/Band Pass Filter
- Variable Gain Amplifier per usare la dinamica dell'ADC

Digital Signal Processing

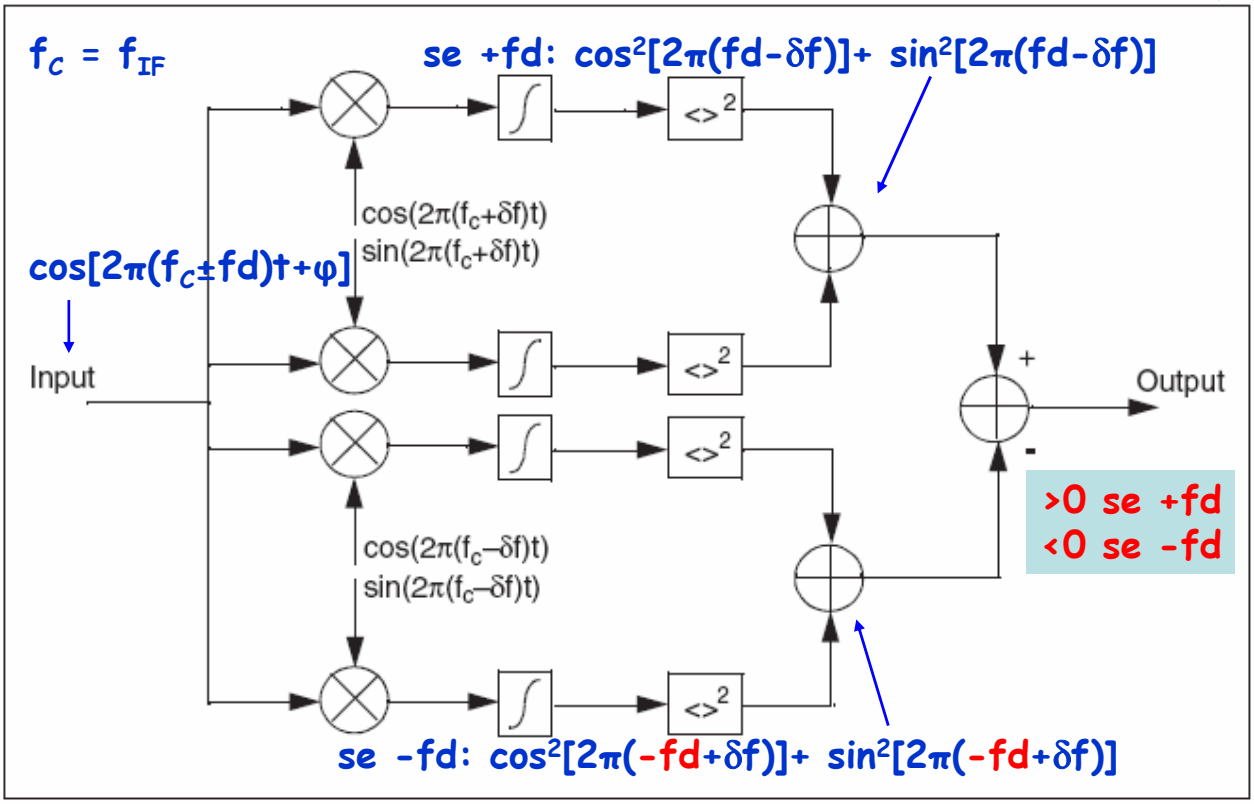


- Il segnale in ingresso del DSP è a IF (< 3 MHz)
- La demodulazione avviene nel DSP, e puo' essere
  - coerente (CPFSK)
  - non coerente (in figura) – richiede meno logica – costo piu' basso

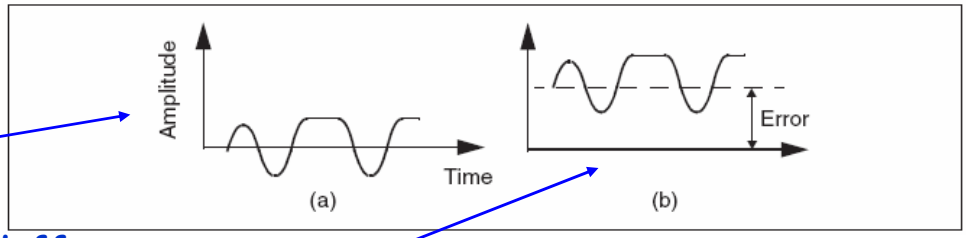
δf = 140 KHz

Ricevitore non coerente

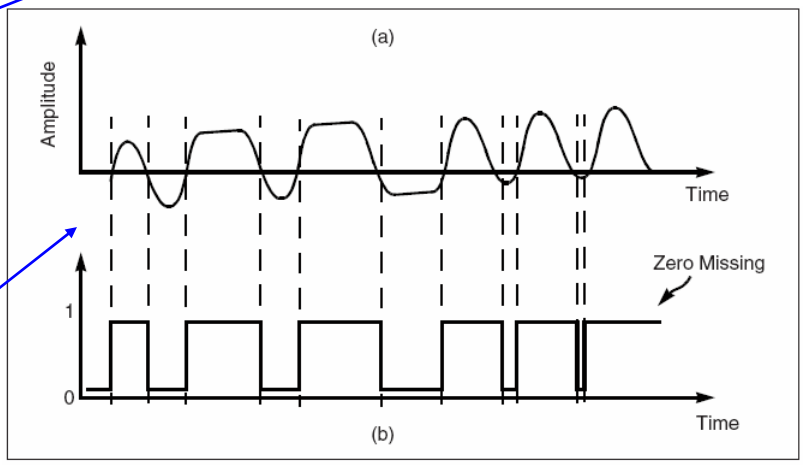
δf = 140 KHz, 115 KHz≤fd≤175 KHz → $|fd - \delta f| \leq 25$ KHz=1/40μs



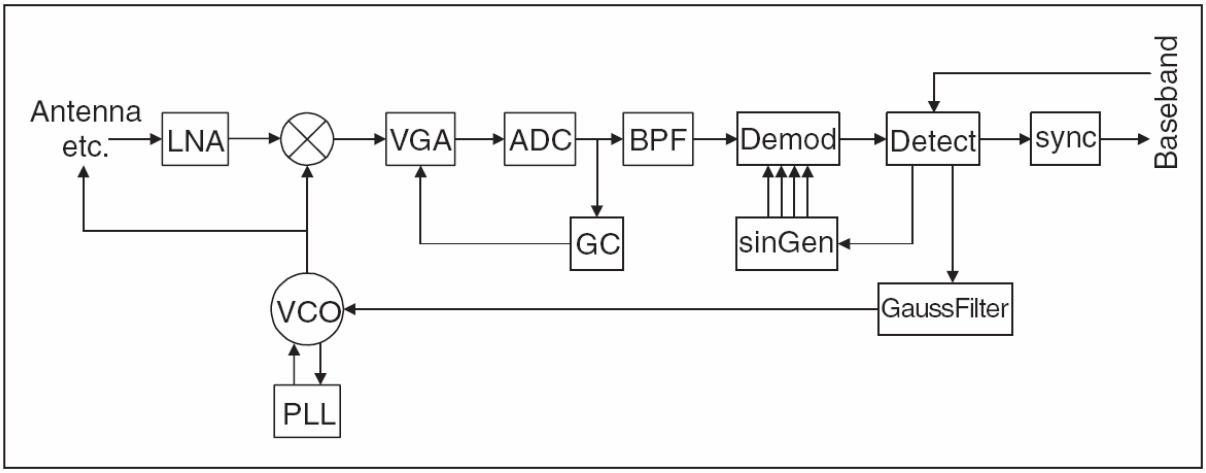
Ricevitore non coerente



- Uscita ideale
- Problema se l'offset è vicino al massimo (150 KHz) e la modulazione è inferiore a 150 KHz. In tal caso il segnale rimane sempre dello stesso segno
- Anche la deriva puo' creare lo stesso problema, verso la fine del pacchetto

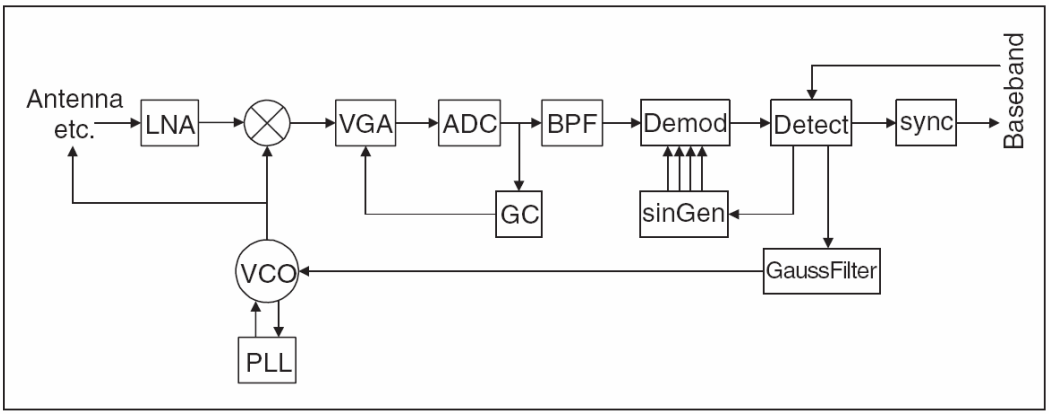


Catena di ricezione
Correzione della frequenza



- BPF – BandPass filter fa passare solo il canale desiderato
- le funzioni di base (fc ± δf in fase e quadratura) sono ottenute in SinGen
- Il detector rileva l'errore in frequenza e manda un segnale di reazione a SinGen. Questo controllo basta se non ci si avvicina troppo al canale adiacente
- In tal caso, il detect manda un segnale

Catena di ricezione
Correzione della frequenza



- le funzioni di base (fc ± δf fase e quadratura) ottenute in SinGen
- Il detector rileva l'errore in frequenza e manda un segnale di reazione a SinGen.
- In caso di errore molto ampio, il detector manda un segnale di incremento ± 75 KHz al VCO attraverso il Filtro Gaussiano (catena di trasmissione)
- L'anello esterno viene bloccato dopo una ampia correzione per evitare instabilità