Bluetooth:
Una interfaccia wireless per la connettività in ambito short-range.

Corso Reti di Calcolatori

Prof. Orazio Mirabella

Introduzione

- Nel febbraio 1998 Ericsson, Nokia, IBM, Toshiba e INTEL formarono uno "Special Interest Group" (SIG) per creare uno standard wireless per la connettività in ambito "short range".
- L'interfaccia radio fu chiamata Bluetooth dal nome del re danese Harald Bluetooth che aveva riunito danimarca e Norvegia durante il X secolo.
- Questo gruppo fu successivamente esteso nel dicembre 1999 a 3Com, Lucent, Microsoft e Motorola. Attualmente, oltre 2000 aziende sono entrate nel consorzio di utenti della tecnologia Bluetooth.

Cosa è Bluetooth

- Bluetooth è una interfaccia wireless a corto raggio per il trasferimento di voce e dati punto-multipunto, fra dispositivi portatili
- Il range nominale varia da 10 cm a 10 metri ma può essere esteso a 100 metri aumentando la potenza di trasmissione.
- Printers, desktops, fax machines, cellular phones e virtualmente ogni altro tipo di dispositivo digitale può fare parte del sistema bluetooth per formare dei gruppi che sostituiscono i cablaggi.

Goals

- Il sistema deve essere capace di supportare una connettività peer-to-peer operando con una struttura ad-hoc.
- La connessione deve supportare sia voce che dati.
- Deve presentare una elevata immunità ai disturbi generati da altri dispositivi.
- Il transceiver radio deve essere abbastanza piccolo da operare a bassa potenza e poter essere integrato in dispositivi portatili di piccola dimensione come telefoni cellulari, auricolari, computer palmari, ecc.
- Deve avere un basso costo (5$ per chip)

Scenari applicativi

- ***3-in-1 phone***: A casa usato come telefono mobileA (al costo della telefonia fissa), nell'uso esterno come telefono cellulare (costo telefonia mobile), e quando il telefono è nell'area di un altro telefono mobile, usato come walkie-talkie (senza costi telefonici).
- ***Ultimate Headset***: per collegare l'auricolare wireless al telefono cellulare, al notebook o altri dispositivi.
- ***Interactive Conference:*** per riunioni e conferenze.
- ***Automatic Synchronizer***: Per sincronizzare le attività di diversi dispositivi come desktop, notebook, palmare e telefono cellulare.
- ***LAN access***:. per consentire l'accesso a internet attraverso un telefono cellulare o un modem cordless.
- ***E ancora:*** *per creare reti diffuse di sensori, per applicazioni di controllo di processo, per la home automation, ecc.*

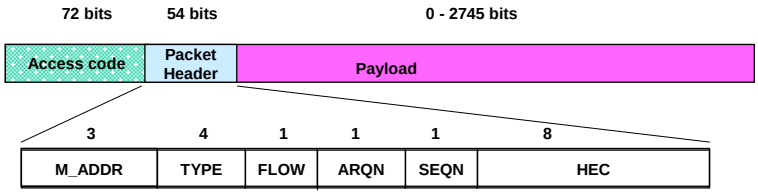
Alcune definizioni

- Piconet: una collezione di dispositivi (fino ad 8) connessi attraverso bluetooth in modo da formare una rete ad-hoc. Ogni piconet possiede una diversa sequenza di hopping cui si sicronizzano tutti gli host della piconet.
- Scatternet: due o più piconet indipendenti e non sincronizzate che comunicano l'un l'altra.
- Master unit: è il dispositivo che in una piconet fornisce il clock e la sequenza di hopping cui tutti i dispositivi della piconet.
- Slave units: tutti i dispositivi della piconet che non sono il master (fino a 7 unità attive per ogni master)

L'interfaccia wireless di Bluetooth

- Opera nella banda Industrial-Scientific-Medical (ISM), a 2.45 GHz che è libera nella maggior parte dei paesi del mondo.
- Utilizza la modalità Frequency-hopping (FH) spread spectrum, che permette di supportare implementazioni low-cost, low-power radio con elevata immunità alle interferenze.
- I canali usano uno schema Frequency-Hopping/ Time Division Duplex (TDD): il canale è diviso in slot di 625μs con 1600hops/sec. Gli slot consecutivi sono usati alternativamente per trasmettere e ricevere.
- Ogni slot consente di trasmettere un solo pacchetto.
- Il canale trasmissivo fa uso di 79 canali da 1-MHz, ugualmente spaziati, (da 2,402 MHz a 2,480 MHz), con modulazione di tipo frequency shift keying (FSK). Il bit rate di trasmissione/ricezione è 1 Mb/s
- Sono usati 2 livelli di potenza: 0dBm per 10 metri o 20dBm (100 metri)

Struttura del pacchetto

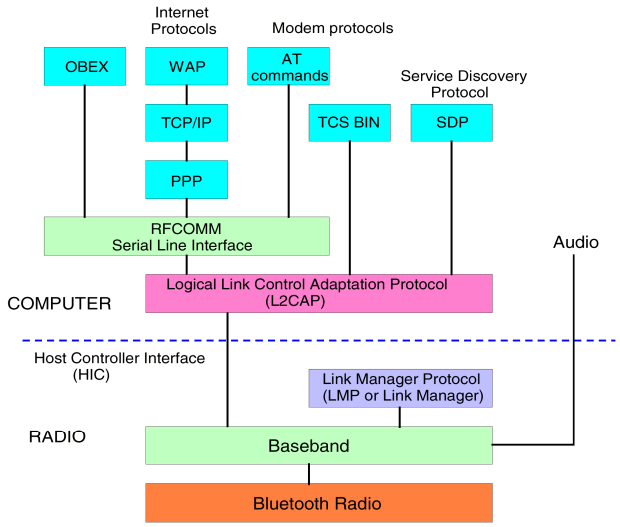


- Un access code di 72-bit, unico per il canale , è usato per l'identificazione del pacchetto e la sincronizzazione col master.
- Header: 3-bit slave address, packet type, flow control bits, ARQ bit, sequence number, Header-Error-Check fields.
- Payload: 0-2745 bits
- Sono stati definiti anche dei pacchetti Multislot: un pacchetto può coprire uno, tre, cinque slot e viene trasmesso con un singolo hop in frequenza del canale.

Link supportati

- Sono disponibili due tipi di link per applicazioni multimediali:
  - Synchronous Connection-Oriented (SCO) link
  - Asynchronous Connectionless Link (ACL)
- I link SCO supportano connessioni, circuit-switched point-to-point simmetriche usate tipicamente per la voce.
  - La prenotazione può essere effettuata dal master o dallo slave
- I link ACL supportano connessioni packet-switched point-to-multipoint usate tipicamente per la trasmissione di dati bursty.
  - Le unità Master usano uno schema a polling per controllare le connessioni ACL: si usa un pacchetto master-to-slave o un pacchetto di tipo POLL per interrogare lo slave. In tal modo vengono evitate le Collisioni.
- Tutto il traffico di tipo SCO e ACL è schedulato dal master

Architettura



RF e Baseband

Rappresentano la parte più a basso livello del protocollo:

- Implementano in hardware le funzioni necessarie per la realizzazione di link wireless
- Controllano la sincronizzazione fra le varie unità e la corretta sequenza di hopping.
- Comprimono i dati e li inseriscono nei pacchetti.
- Assegnano gli identificatori
- gestiscono i link di tipo SCO ed ACL
- Curano la ritrasmissione dei pacchetti errati e la rivelazione/recupero degli errori.

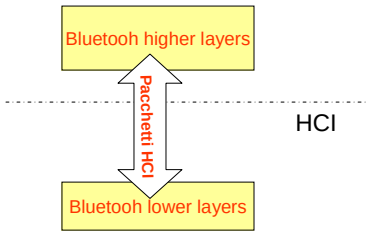
Link Manager Protocol (LMP)

E' responsabile per:

- Instaurazione della connessione
- Generazione, scambio e controllo del link e delle chiavi criptate per l'autenticazione e la criptazione dei dati.
- Negoziazione delle modalità operative del Link. Cioè voce/dati
- Spedizione e ricezione dei dati
- Management delle modalità operative in potenza, del consumo di potenza e dello stato di una unità.

Host Controller Interface

- Poiché la maggior parte dei sistemi Bluetooth hanno Baseband e Link Manager su un processore e gli altri livelli e le applicazioni su un altro processore, è necessario definire una interfaccia standard fra i due.
- Una interfaccia standard permette di utilizzare drivers di costruttori diversi e quindi di fare uso di moduli Hardware bluetooth di costruttori diversi



Sono disponibili diversi tipi di pacchetti:

Command packets

Event packets

Data packets

Logical Link Control and Adaptation Protocol (L2CAP)

- L2CAP è una interfaccia fra i protocolli dei livelli superiori ed il livello baseband. Opera in parallelo al LMP
- Multiplexing: L2CAP deve supportare il multiplexing fra vai protocolli (ad es. SDP, RFCOMM and TCS Binary) che possono operare sul L2CAP.
- Segmentation and Reassembly: Data packets che superano la Massima Transmission Unit, MTU, devono essere segmentati prima di essere trasmessi. In ricezione devono essere riassemblati da L2CAP.
- Quality of Service: La connessione L2CAP permette lo scambio di informazioni relative alla qualità di servizio fra due unità bluetooth.

Service Discovery Protocol (SDP)

- Definisce il modo in cui una applicazione "client" opera per scoprire i servizi forniti dal Bluetooth servers (quali printing, file transfer, synchronization) e le loro caratteristiche.
- Definisce come un "client" può cercare un servizio, sulla base di attributi specifici, senza conoscere nulla sui servizi disponibili
- Fornisce i mezzi per la scoperta di nuovi servizi che divengono disponibili quando il client entra un'area dove opera un server Bluetooth.
- Fornisce le funzionalità per determinare quando un servizio non è più disponibile.

RFCOMM

Una porta RS232 ha nove linee usate per trasferire dati e segnali di controllo.

RFCOMM emula il collegamento RS232 per connettere il livello Baseband con una applicazione finale utente o con una applicazione intermedia. Sono supportati due tipi di dispositivi:

- oTipo 1: porta seriale emulata per dispositivi terminali di un communication path quali un PC o una stampante.
- oTipo 2: porta seriale fisica di dispositivi intermedi in un communication path quale ad esempio un modem.

Il protocollo usato è il GSM TS 07.10 usato per i telefoni cellulari per multiplexare diversi data stream su una singola connessione fisica. Sono usati cinque tipi di frames:

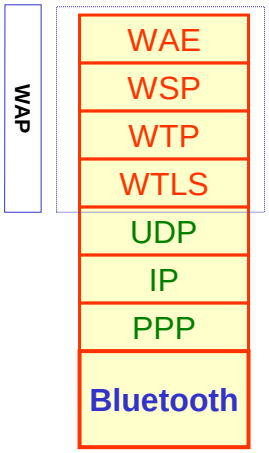
- oSABM- Start Aynchronous balanced mode (comando di start-up)
- oUA - Unnumbered Acknowledge (Risposta dopo la connessione)
- oDISC - Disconnect (comando per la disconnessione)
- oDM - Disconnect Mode (in risposta ad un comando)
- oUIH - Unnumbered Information with Header check.

Wireless Access Protocol(WAP)

- Il **WAP** è un protocollo wireless per consentire ai dispositivi mobili di usare i servizi disponibili su Internet.
- WAP opera con diverse tecnologie wireless che supportano la comunicazione (CDMA, GSM, DTMA, DECT, ecc.). Attualmente non è attiva una collaborazione formale fra WAP forum e Bluetooth S.I.G.
- **WAP supporta una comunicazione Client-Server**. Un dispositivo client WAP-enabled usa un micro-browser, specificamente progettato per operare con dispositivi con schermi di piccola dimensione e poca memoria.
- Il linguaggio usato è il **Wireless Markup Language** (WML) simile ad HTML ma adatto per piccoli monitor.
- I destinatari ideali del WAP in applicazioni bluetooth non sono comunque i cellulari ma i Palmari (Pocket PC).

Lo Stack WAP

- WAP usa una combinazione di Internet Protocols (quale UDP) e protocolli specifici per uso mobile.
- WAE, Wireless Application Environment: fornisce una user interface (tipicamente un micro browser).
- WSP, Wireless Session Protocol: supporta una sessione fra il client WAP ed il server WAP.
- WTP, Wireless Transport Protocol: fornisce un Transport layer affidabile per il WSP. Superfluo se usato con Bluetooth.
- WTLS, Wireless Transport Layer Security: Fornisce sicurezza. Può essere omesso con applicazioni che non necessitano di una sicurezza maggiore di quella fornita da Bluetooth.
- Il PPP, Point to point Protocol fornisce un trasporto di pacchetti client/server e si usa normalmente col telefono. E' giustificato dall'uso della sottostante connessione seriale RFCOMM

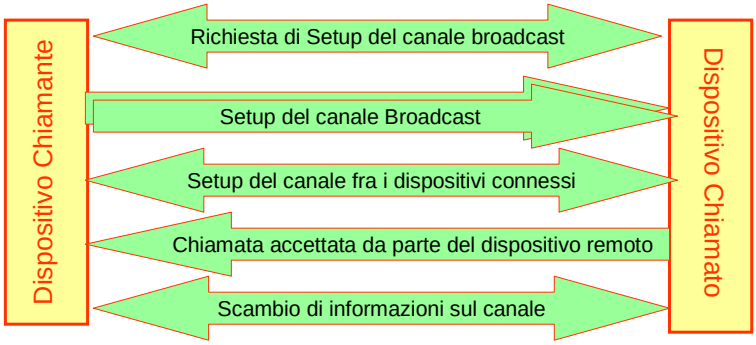


OBEX

- OBiect Exchange (OBEX) è un protocollo binario progettato per consentire a vari dispositivi di scambiare dati semplicemente e spontaneamente.
- L'architettura è di tipo Client/Server per permettere ad un client di chiedere/inviare dati ad un server.
- OBEX è uno standard IrDA(infrared Data Association) molto adatto a trasferire dati fra dispos itivi Bluetooth (le modalità operative IrDA e Bluetooth sono molto simili).
- OBEX si mappa su RFCOMM (opzionalmente su TCP/IP). In ogni dispositivo occorre un canale RFCOMM per ogni server OBEX attivo.
- Le applicazioni Server OBEX devono registrare i loro servizi nel Database del Service Discovery.
- Usa comandi semplici: Connect, Disconnect, Put, Get, Setpath, Abort.

Telephony Control protocol - TCS

- Definisce le modalità per inoltrare telefonate sia punto-punto che multipunto, attraverso Bluetooth.
- Le telefonate multipunto si verificano quando più utenti possono rispondere ad una telefonata (es. telefono di casa).
- I messaggi di segnalazione del TCS sono inviati come payload dei pacchetti L2CAP.



Bluetooth Networking

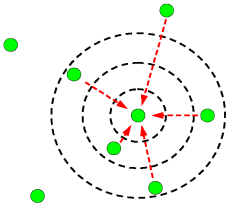
- **Le Piconet sono costituite da fino a 7 dispositivi attivi.**
  - Configurazione Master/Slave
  - Slave addizionali possono essere posti in Parked mode. I dispositivi non sono attivi ma rimangono sincronizzati.
  - Le connessioni, sincronizzazioni e stati Parked/Active sono controllati dal Master.
  - Tutti i dispositivi connessi ad una Piconet condividono tempo e frequenza.
- **Una Scatternet è formata da due o più Piconet.**
  - Si ha un Master per ogni Piconet. Un Master può essere Slave di un'altra Piconet.
  - Gli Slave afferenti a più Piconet sono multiplexati nel tempo.
  - Differenti Piconets non sono sincronizzate né in tempo né in frequenza.

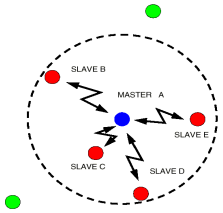
Stabilire una connessione

- Quando le unità non sono connesse, si trovano in STANDBY mode, dove ciascuna di esse ascolta su 32 wake-up channels, (unici per ogni unità) per messaggi di page o inquiry.
- Gli intervalli di Wake-up variano fra 0 e 3.84s (usualmente 1.28s)
- Una unità entra nello stato di PAGE o INQUIRY in cui essa broadcast messaggi di page o inquiry.
- Se la paging unit conosce l'identità dell'unità con cui vuole connettersi, allore conosce la sequenza di wake-up e trasmette ogni 1.25ms il codice d'accesso dell'unità, su 16 differenti frequenze di hop definite per l'unità slave (il periodo totale è 10ms)
- Se il pager non conosce l'identità dell'unità, allora (per un tempo che va da 0 a 2.56s) invia in broadcasts un messaggio di inquiry in accordo ad una sequenza comune di inquiry.

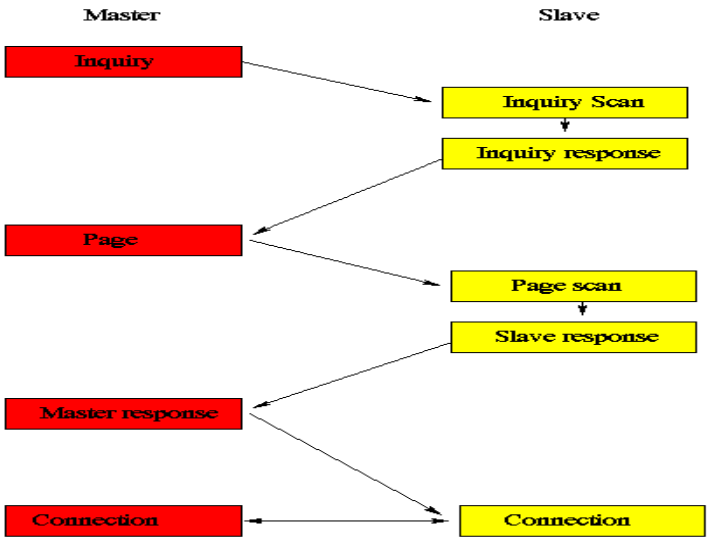
Stabilire una connessione

- Per stabilire una connessione ogni unità trasmette un messaggio Inquiry per scoprire tutte le unità esistenti nella Piconet.
- Una unità diviene il Master, e le altre Slave.
- La relazione Master/Slave stabilisce le temporizzazioni.
- Un Master può divenire lo Slave in un'altra Piconet. In tal modo le due Piconet formano una Scatternet.



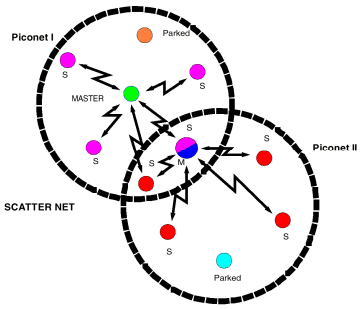


Stabilire una connessione



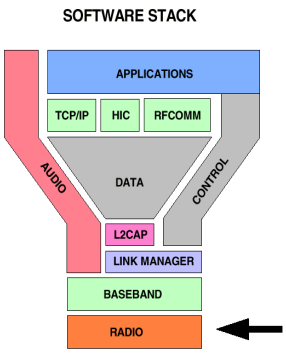
Piconet e Scatternet

- Il Master in una Piconet può essere Slave in un'altra.
- Problemi di indirizzamento limitano il numero di dispositivi attivi in una piconet a 7.
- Un numero indefinito di dispositivi Parked rimangono sincronizzati con la piconet ma non sono attivi.



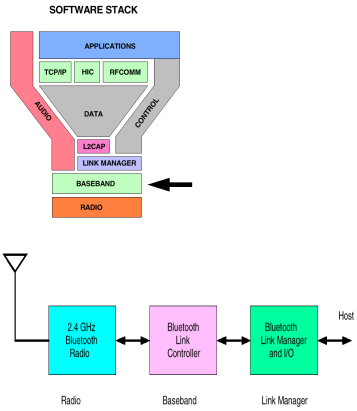
Bluetooth Radio

- Il range usato è 2400-2483,5 Mhz accettato in quasi tutto il mondo.
- 1600 hops/sec in frequenza (ogni 625μSec)
- 79 canali da 1MHz (23 in Francia)
- Time Division duplex
- Tx power variabile fra 0 dBm a 20 dBm
- Range da 10 Cm a 10 metri (a 0 dBm)
- Data rate variabili fra 108/108 kbps per canali simmetrici a 723/57 kbps per canali asimmetrici
- Trasmissione isocrona (di tipo circuit switched) o asincrona (tipo Packet switched).



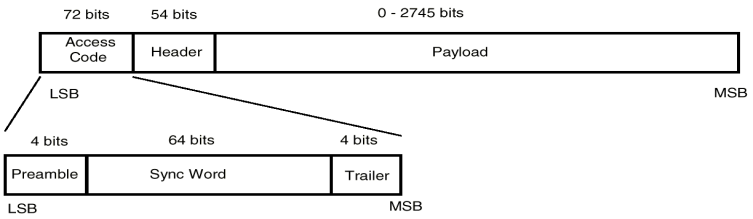
L'obiettivo è la realizzazione di un singolo Chip a basso costo

Bluetooth Baseband



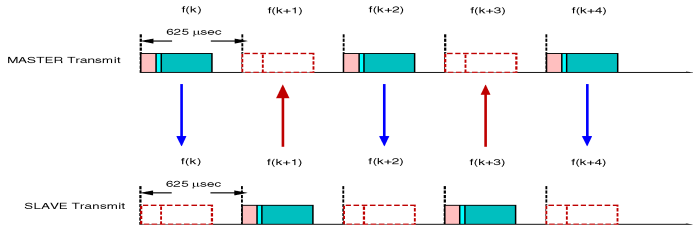
- Frequency Hop Time Division Duplex channel
- Il canale è basato su slot di 625µSec di cui 220 µSec sono persi per agganciare il PLL.
- Sono supportati:
  - fino a tre canali vocali simultanei da 64Kbps.
  - Canali voce simultanei a canali dati
  - canali dati asincroni

Bluetooth Baseband



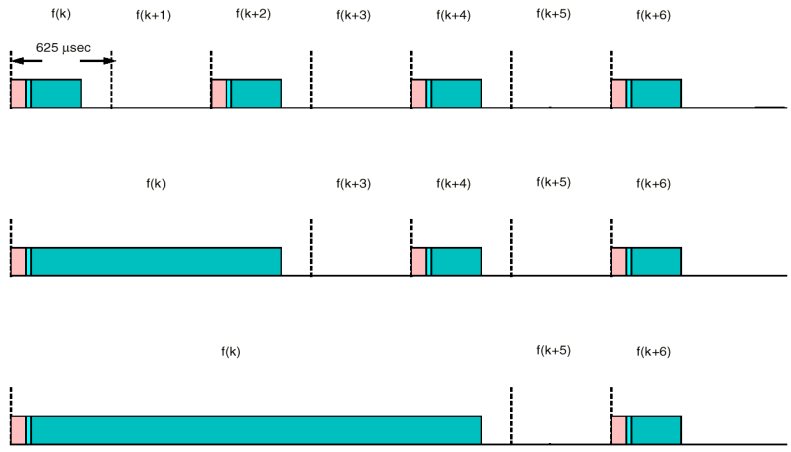
- Channel Access Code (CAC): identifica una piconet. E' usato con tutto il traffico scambiato su una piconet.
- Device Access Code (DAC): è usato per la segnalazione cioè per effettuare il paging o per rispondere ad un paging.
- Inquiry access code (IAC): Codice di access generale usato per l'inquiry.

Temporizzazione dei pacchetti



- Time Division Duplex (TDD)
- Circa 229 µsec sono persi per agganciare il sintetizzatore. Ciò permette di usare semplici circuiti di PLL.
- Il Master trasmette negli slot pari.
- Lo slave trasmette negli slot dispari.
- Ogni slot può trasmettere al più un pacchetto
- La frequenza degli slot cambia in accordo ad una sequenza prestabilita.

Pacchetti multi-slot



Tipi di pacchetti: di sistema

- ID: contiene il device access code o l'inquiry access code. E' usato per il paging, inquiry e come risposta.
- NULL: contiene il channel access code ed il packet header usato per gli ack e controllo di flusso.
- POLL: Simile al Null, ma è richiesta la risposta da parte di uno slave dopo la ricezione.
- FHS: contiene il Bluetooth device address ed informazioni sul clock del mittente usate per il setup di una piconet e per la sincronizzazione degli hop.

High Quality Voice Packets

- HV1 Packet:
  - protetto da un Forward Error Correction (FEC) con rate 1/3. Nessuna ritrasmissione né CRC.
  - 10 bytes dati, 1,25 msec di voce a 64Kbps
  - Ritrasmissione ogni 2 time slot.
- HV2 Packet:
  - protetto da un Forward Error Correction (FEC) con rate 2/3. Nessuna ritrasmissione né CRC.
  - 20 bytes dati, 2,5 msec di voce a 64Kbps
  - Ritrasmissione ogni 4 time slot
- HV3 Packet:
  - Nessuna protezione con FEC. Nessuna ritrasmissione né CRC.
  - 30 bytes dati, 3,75 msec di voce a 64Kbps
  - Ritrasmissione ogni 6 time slot.
  -

Data Packets

Medium rate error protected

- DM1: 18 bytes dati; occupa 1 slot; 2/3 FEC + CRC a 16 bit
- DM3: 123 bytes dati; occupa 3 slot; 2/3 FEC + CRC a 16 bit
- DM5: 226 bytes dati; occupa 5 slot; 2/3 FEC + CRC a 16 bit

High data rate, no error protection.

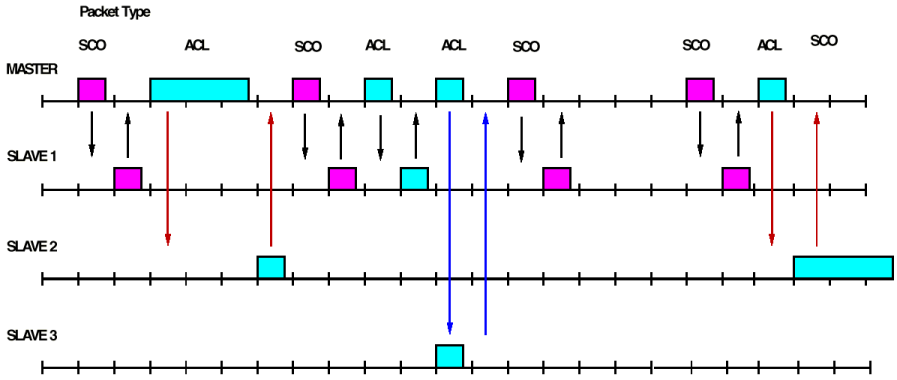
- DH1: 28 bytes dati; occupa 1 slot; nessun FEC; CRC a 16 bit
- DH3: 185 bytes dati; occupa 3 slot; nessun FEC; CRC a 16 bit
- DH5: 341 bytes dati; occupa 5 slot; nessun FEC; CRC a 16 bit

LINK FISICI

- Asynchronous connectionless Link (ACL):
  - Il master scambia pacchetti con ogni slave (uno per slot)
  - Connessioni packet switched con tutti gli slave attivi nella piconet.
  - Solo un ACL per ogni slave
  - I pacchetti non indirizzati ad uno specifico slave sono spediti in broadcast e letti da tutti gli slave.
- Synchronous Connection Oriented (SCO) link:
  - Link simmetrico punto-punto fra master ed uno specifico slave.
  - Connessioni di tipo circuit switched con time slots riservati.
  - Un master può supportare fino a 3 link SCO contemporaneamente.
  - Uno slave può supportare fino a 3 link SCO con un master o 2 con master differenti.
  - Il livello di Link Manager (LM) stabilisce i link SCO mediante i messaggi del protocollo di LM

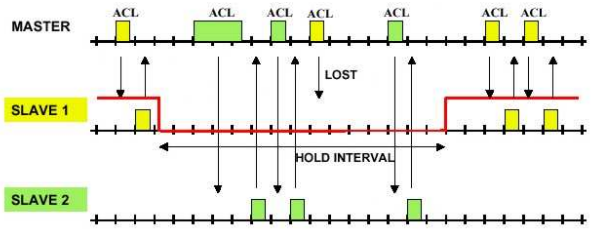
Link multipli con pacchetti misti

Diversi tipi di link possono coesistere in una piconet



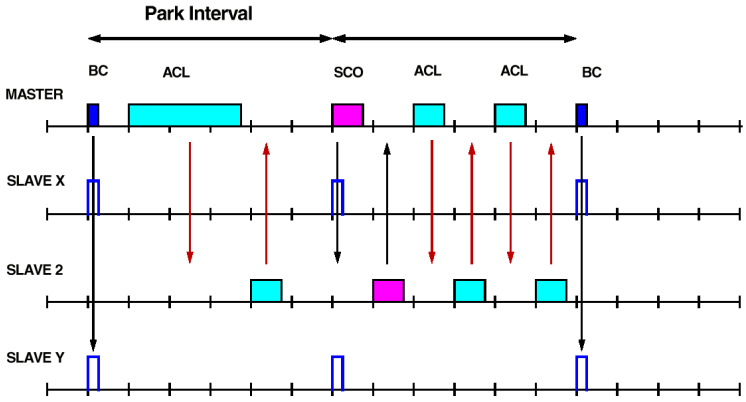
HOLD mode

- E' una modalità di risparmio di energia può essere usata per connettere le unità in una piconet se non deve essere trasmesso alcun dato.
- Il master può mettere l'unità slave in Hold Mode, in cui è attivo solo un timer interno. Le unità slave possono comunque chiedere di essere poste in Hold Mode.
- Il trasferimento dati ricomincerà istantaneamente quando le unità escono da questo stato.



PARK mode

- I dispositivi sono addormentati e si risvegliano periodicamente per risincronizzarsi
- il numero di dispositivi può essere elevato (cioè > 7).
- Ogni dispositivo riceve un codice di 8 bit:Park Member Address



SNIFF mode

- Il dispositivo rimane attivo ma con un duty-cycle ridotto.
- L'intervallo di sniff è programmabile e dipende dall'applicazione.
- Può essere risvegliato in corrispondenza degli intervalli di sniff.