Bluetooth

Estados de dispositivos bluetooth:

Standby → waiting to join picouet

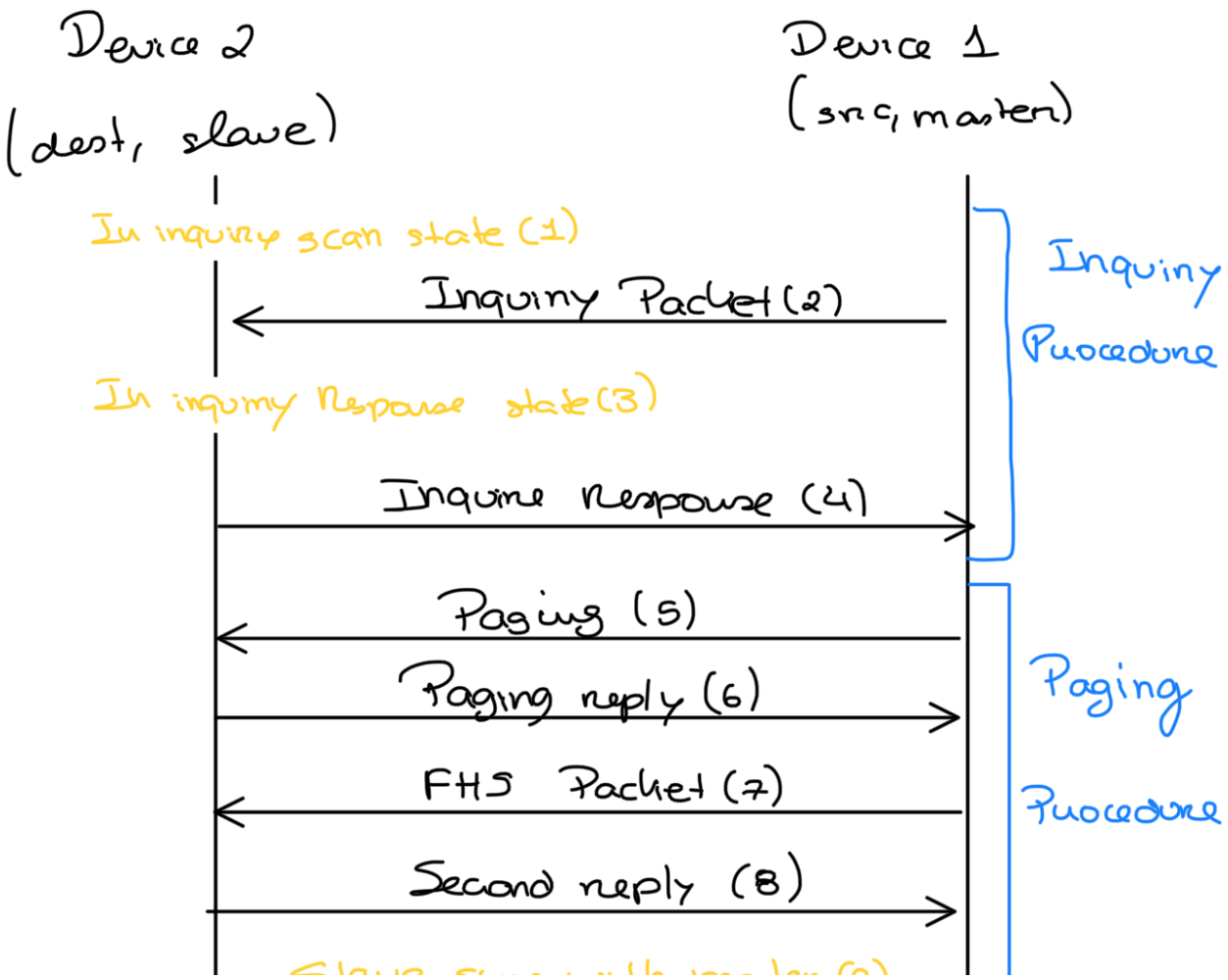
Inquire → ask about radios to connect

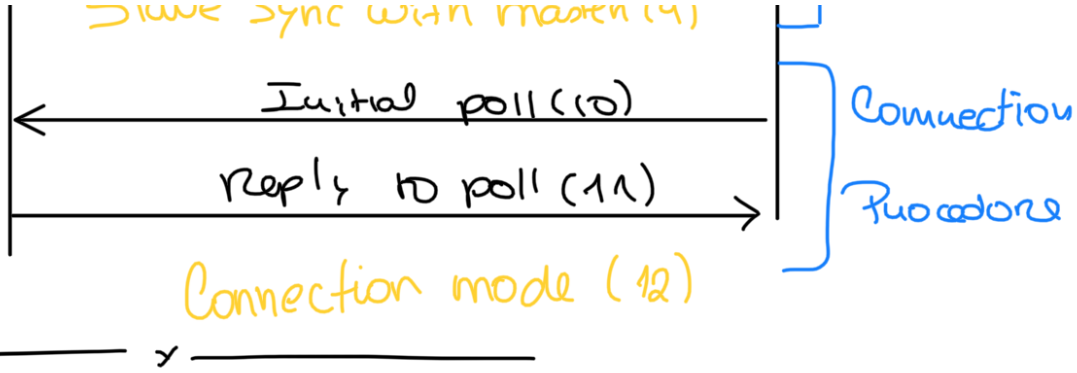
Page → connect to a specific radio

Connected → actively on a picouet (master or slave)

Park/sniff/Hold → low power connected states.

Connection procedure





A. Scan

4. Protocol: HCI_CMD (Host controller interface)

(host → controller)

HCI_EVT

(controller → host)

5. 1° sent inquiry → 0,2756 → inquiry cancel (10,1s)

LE

2° sent inquiry 10,24s → inquiry complete (20s)

3° sent inquiry 20,6s → inquiry complete (30s)

4° inquiry 31s → inquiry complete (41s)

5° inquiry 40s → inquiry complete (51s)

(host → controller) (controller → host)

Isto pois o inquiry tem um parametro inquiry length (~10 seg.)

8. Read features: class, supported commands, ...

... supported commands, codecs, buffer size,

write class, connection, link policy, inquiry mode, pairing mode, etc.

set scan enable and parameters, event

B. Pair, connect and use (mouse)

12. Protocols: ATT (Attribute protocol) → bidirectional

HCI_CMD / EVT (CMD → host → hp)
(EVT → hp → host)

L2CAP (logical link Control and Adaptation protocol):
bidirectional, send connection parameters

SMP (Security Management Protocol):
bidirectional, identity info, encryption, pairing

13. Sequencia de events:

(...)

host → controller (LE Create connection 0x08|0x000d)

host → controller (read remote features)

PC → HP ...

pairing request (Protocolo SMP)

(Auth, bonding, secure connection, keys)

host → controller → Start Encryption (HCI_CMD

14. Apenas ATT (info sobre mouse movements)

→ Também pode ter um handle de battery level (54%)

→ Mouse clicks são os 2 valores mais significativos do código hex mandado.

→ Movement são os 6 do meio.

16. A disconexão é feita onde o controller manda um HCI_EVT com (Disconnect complete)

C. Pair, connect and use (headphones)

18. Protocolos envolvidos: (m

- HCI_CMD/EVT
- L2CAP (logical link control and adaptation protocol)
  - vai dentro do HCI ACL
- SDP (Service discovery protocol)
  - vai dentro do L2CAP
- RFCOMM (Radio Frequency communication)

- vai dentro do L2CAP
- Info sobre o canal (mudança do canal O para o 10 pelo host)

- HFP (Hands-Free Profile)
  - vai dentro do RFCOMM
  - inclui AT + BRSF

- AVDTP (Audio/Video distribution transport protocol)
  - Vai dentro do L2CAP (info de audio e headset)
  - contém info sobre configurações, media codec, joint stereo, block, subbands, loudness).

- SBC (Sub-band coding)
  - vai dentro do RTP, que vai dentro do A2DP, que vai dentro do L2CA

- AVRCP (Audio/Video Remote Control Profile)
  - vai dentro do AVDTP
  - Mudanças de volume (percentagem de volume
  - Mudanças de música (seguinte, etc)
  - Play / Pause
  - Mudança de player

D. Connect and unpair (headphones)

- Connection request por parte do host

e aceitação por parte do headset (info em pacotes HCI).

. Disconnect request por parte do host para o fones.

E. Audio call (Messenger)

- O host sai do modo de sniffing, low power, a ver se há conexões
- Está a ser feita uma conexão sincronizada
- Depois é enviado informação sincronizada

Protocolo HCI-H4 (Synchronous Data : type = 0x03)
Asynchronous Data: 0x02
Command : 0x01
Event : 0x04)

↳ Cada dado tem 24 bytes de info
↳ Frequência ~ 600 Hz

- No fim, o host manda um Disconnect por HCI.

F. Audio Streaming (Spotify)

33. Protocolo HCI_H4 → asynchronous data (0x02)
(Antes disso houve mudança de modo através de um comando (0x04)

34. L2CAP → localhost → remote

39. Há uma mudança de modo, os headsets saem de sniff mode e o audio continua.

6. Uni and bidirectional audio, microfone

38. a)

Configuração de dois dispositivos (audio)

b) do localhost para o dispositivo. (SBC)

c) Começa-se a receber info (tudo em HCI_H4.