

Bluetooth

→ Personal networks

- No physical access to cabled networks, no need for large communication rates, low cost.

Targets: low power, low cost, short-range, small number of devices.

→ Bluetooth

- Originally for replacing 'USB', not Ethernet.
- PAN → 1 Mbps connections, packet routing, sync and async, voice connections.
- Small, cheap, low power, short-range radios.
- Master/slave config and scheduling.

↳ Bluetooth Higher Speeds.

EDR - Enhanced Data Rate: BT v2.0 → 3 Mbps

HS - High Speed: BT 3.0 HS - 24 Mbps
but data does not go over the BT link itself
it uses 802.11.

↳ Features

2.4 GHz worldwide, airplane friendly, packets and scatternets, 720 kbps, frequency hopping.



↓
signal broadcast over seemingly random series of frequencies. Receiver maps

between freqs. with transmitters

↳ Piconets

- Bluetooth devices connected in ad-hoc cell.
- Master with up to 7 slaves (active) and hundreds parked. Master defines clock and device ID.
- Each piconet has an unique FH pattern.

↳ Scatternet

- Connection of several piconets through common bridge.
- One device can be **PIB** at same time
- piconet BW < 1 Mbps

Master and Slave

→ Piconet Operation

All devices must share the same hopping pattern
If device in piconet and not connected then must be in standby.
2 type of addresses (Active - 3 bits, Parked - 8 bits)

↳ Estados de dispositivos bluetooth:

Standby → waiting to join piconet

Inquire → ask about radios to connect

Page → connect to a specific radio

Connected → actively on a piconet (master or slave)

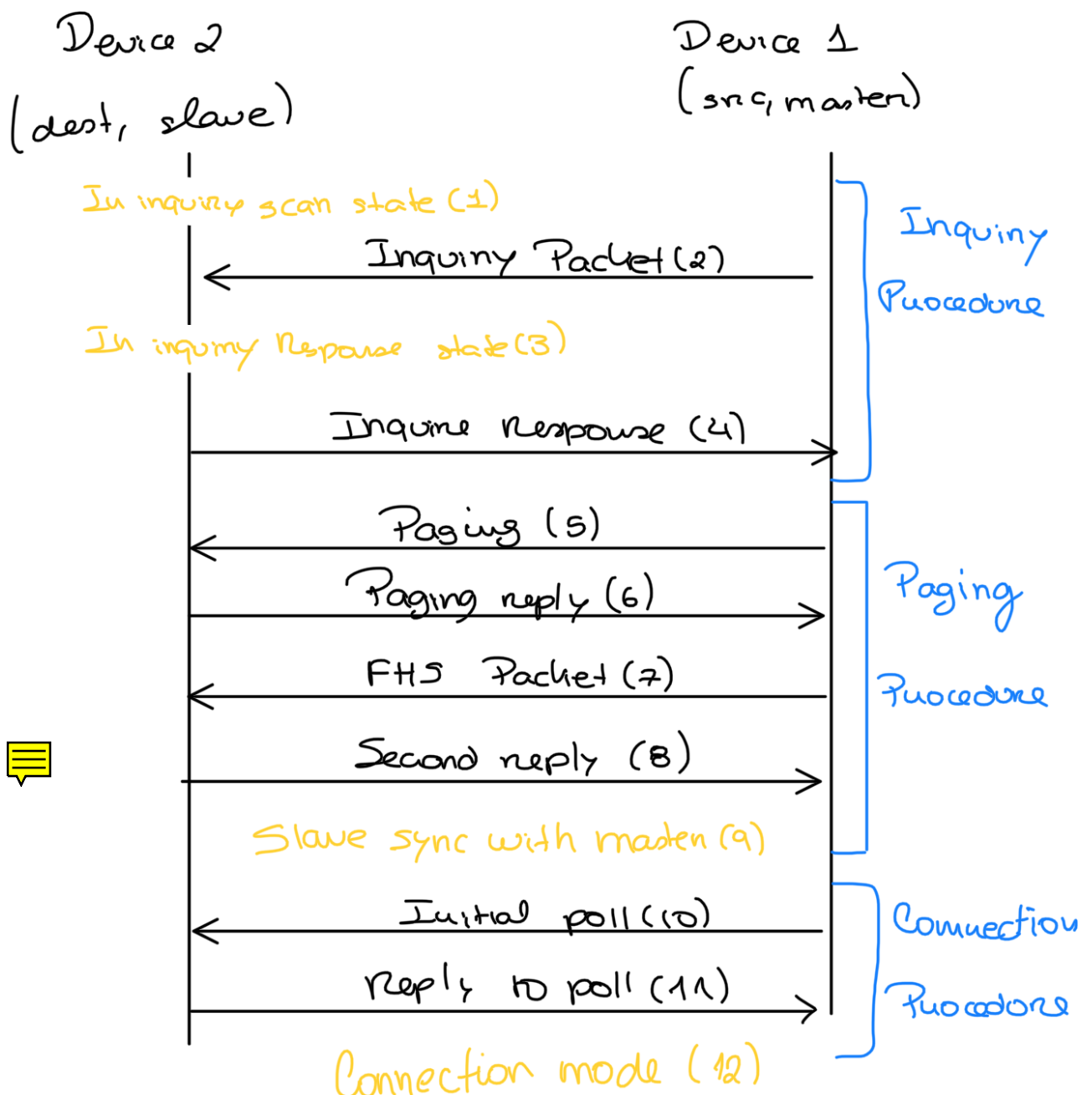
Park/sniff/Hold → low power connected

Very low power
Used to admit more
than 7 slaves.
Wakes up periodically
to listen for broadcasts
to 'unpark'

slave wakes up
periodically to
talk to master,
in sniff intervals.

node sleeps
for defined
interval. No
ACL packets.

Connection procedure



↳ Inquiry Scanning : summary

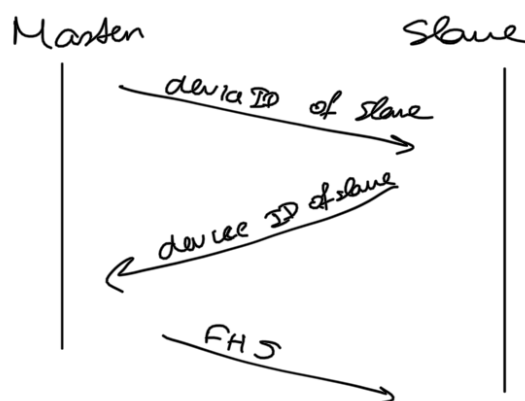
Inquiry scanning has a common address and devices can page this address. All machines hearing an inquiry will answer the inquiry request. There is a detection (connection hit) in the slaves that detects inquiries.

If there is a collision on answering to a scan, they also wait a random period.

↳ Paging.

Very similar to inquiry. Still have not sync clocks or freqs. Establishes actual packet connections (6 step to connect).

FHS packet: contains deviceID and clock (from master).



→ Bluetooth stack



↓
Link Manager and Layer 2 CAP
Radio and Baseband Control

→ Radio layer

Defines requirements for Bluetooth radio transceiver (2.4 GHz band, specs for Spread-Spectrum Frequency Hopping, classify devices).

Frame includes two packets

→ Baseband

Manages physical channels and logical links
Works closely with link controller.

Baseband packet :



↙
channel access
code, device
access code,
inquiry access code.

data

→ Link Manager : carries out link setup with authentication, link configuration

→ Link layer control : link control protocol, connection oriented and connectionless data to upper

layer.

→ HCI : allows command line access to baseband layer and LM for control.

→ Middleware :

- Service Discovery Protocol (SDP) provides a way for apps to detect which services are available and characteristics.

↳ Protocol question ↔ answer

- Protocol message (aims to reuse older protocols)

→ Profiles and security

→ Interoperability : Profiles

Profile : base for BT interoperability, vertical cut in BT stack, a given usage model. Each BT device supports one or more profiles.

→ Security

Level 5: mode 1 → no security

mode 2 → security at service level

mode 3 → security at link level

Mechanisms : fast frequency hopping, low

name, auth, cypher, pin are shared keys.

Link keys in a product: are generated via PIN entry, different for each pair of devices, auth., permanent storage of keys.