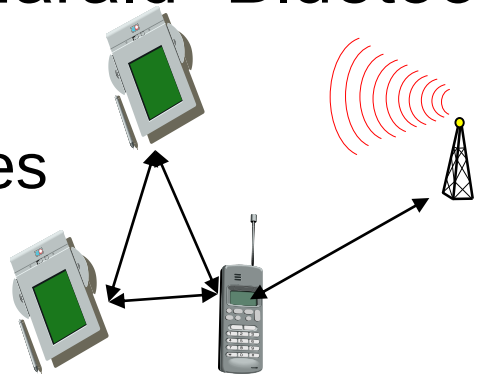
Bluetooth

Connect Without Cables

Bluetooth

- Consortium: Ericsson, Intel, IBM, Nokia, Toshiba - many members
- Named after Denmark king Harald “Bluetooth”
- Scenarios
  - connection of peripheral devices
    - loudspeaker, joystick, headset
  - support of ad-hoc networking
    - small devices, low-cost
  - bridging of networks
    - e.g., GSM via mobile phone - Bluetooth - laptop



- Simple, cheap, replacement of serial and IrDA, low range, lower data rates

Bluetooth evolution

- Bluetooth 1.1 – Standardized as IEEE 802.15.1-2002
- Bluetooth 1.2 - Adaptive Frequency Hopping (AFH)
  - Standardized as 802.15.1 - 2005
- Bluetooth 2 +EDR - Higher speeds (2Mbps, 3Mbps)
  - Through two new modulations – original modulation is GFSK, the new ones are PSK (pi/4 DQPSK and 8DPSK)
- Bluetooth 2.1 – Secure Simple Pairing (SSP)
- Bluetooth 3 +HS – Alternate MAC/PHY (AMP)
  - Uses 802.11 (a/b/g) as an alternate MAC (24Mbps) when lots of data has to be sent. Negotiation of the link, profiles, service discovery and the low power modes are still Bluetooth
- Bluetooth 4 +LE – Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE)

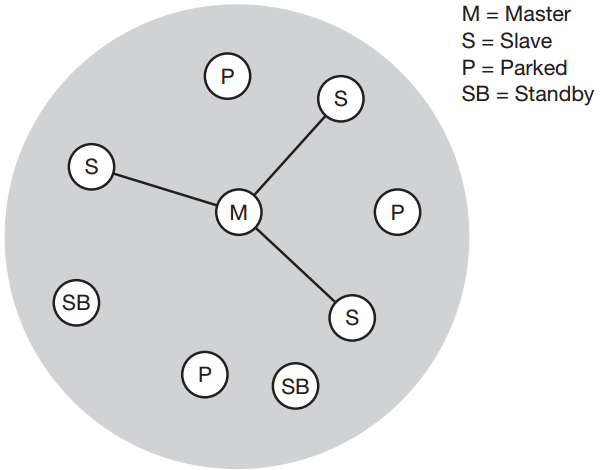
- Introduced in Bluetooth revision 4
- Optimized for low power – *really* low power
- Target: >1 year (4 years possible) on one coin battery cell
  - e.g., CR2032 has 230mAh at 3V
  - The same energy powers a human for 20 seconds
- Other names:
  - Wibree (before adoption by Bluetooth)
  - Bluetooth SMART and Bluetooth SMART READY

Bluetooth 5

- Approved in December 2016 – several enhancements
- Support the emergence of Internet of Things
- Higher speed and longer range compared to Bluetooth 4.x

Networking

- Piconet: a collection of Bluetooth devices that are synchronized to the same hopping frequency.

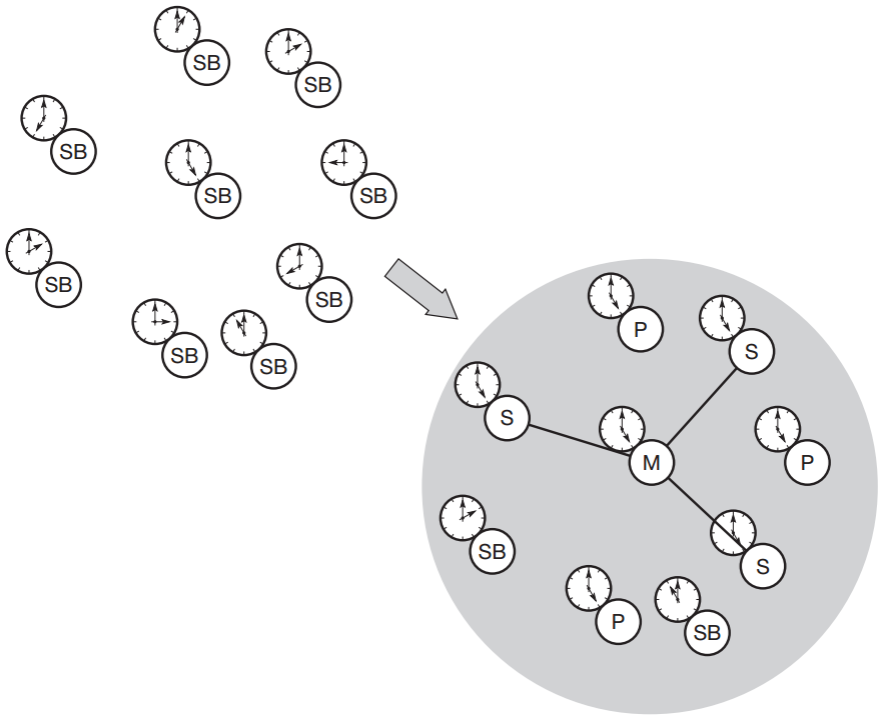


Networking

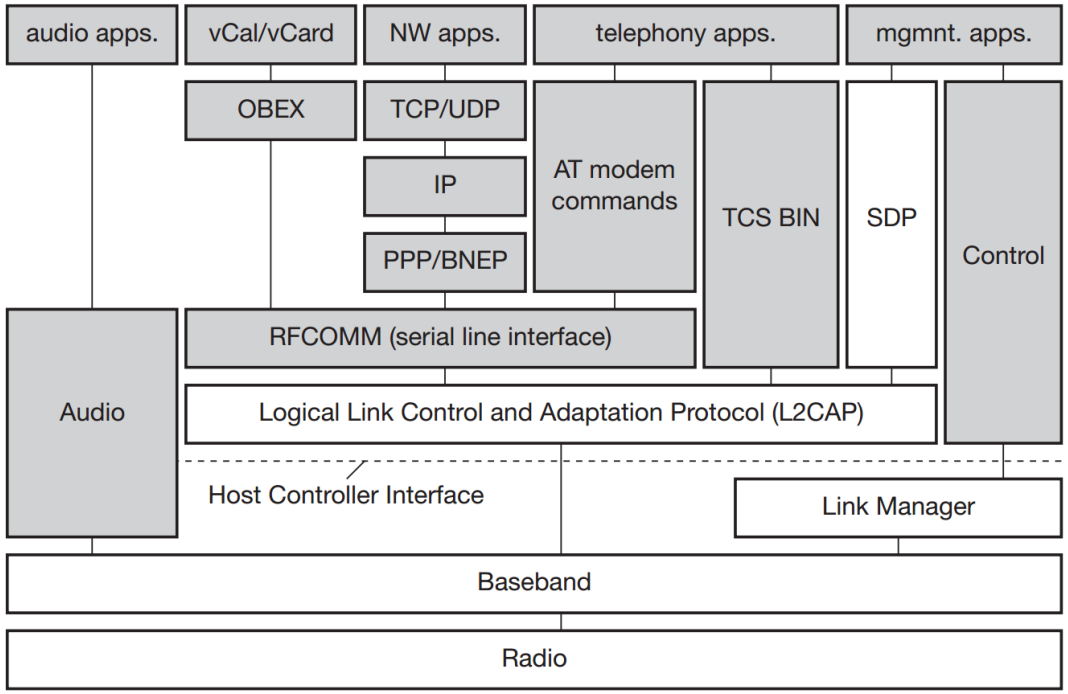
- One device in the piconet acts as the master.
- Other devices act as the slave and connect to the master.
- Up to 7 active members, and 200 stand by members.

Networking

- The master determines the hopping frequency, and slave need to synchronize itself to the master in order to join the piconet.

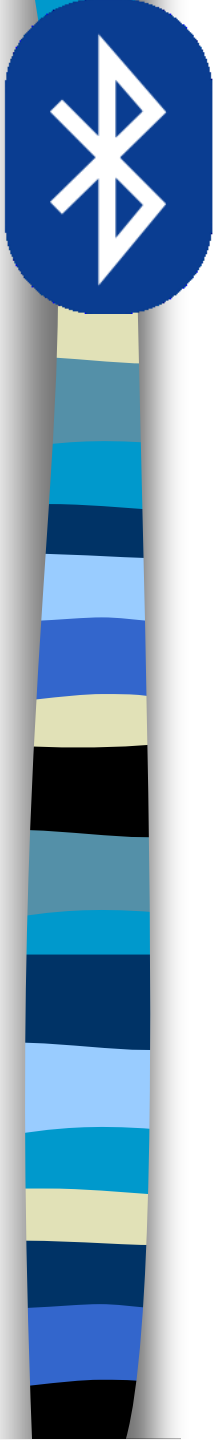


Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol
SDP: service discovery protocol
RFCOMM: radio frequency comm.

Figure 7.44
Bluetooth protocol stack



The **core protocols** of Bluetooth comprise the following elements:

- **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit power (see section 7.5.3).
- **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters (see section 7.5.4).

- **Link manager protocol:** Link set-up and management between devices including security functions and parameter negotiation (see section 7.5.5).
- **Logical link control and adaptation protocol (L2CAP):** Adaptation of higher layers to the baseband (connectionless and connection-oriented services, see section 7.5.6).
- **Service discovery protocol:** Device discovery in close proximity plus querying of service characteristics (see section 7.5.8).

Radio Layer

- Requirement
  - Small, low power.
  - Frequency that is available worldwide.
  - Support of multi-media.
- Implementation
  - 3 power classes
  - 2.4GHz frequency-hopping
    - 1600 hops per second, 625 us per slot.
    - 79 carriers each with 1MHz.

Radio Layer

- **Power class 1:** Maximum power is 100 mW and minimum is 1 mW (typ. 100 m range without obstacles). Power control is mandatory.
- **Power class 2:** Maximum power is 2.5 mW, nominal power is 1 mW, and minimum power is 0.25 mW (typ. 10 m range without obstacles). Power control is optional.
- **Power class 3:** Maximum power is 1 mW.

Baseband Layer

- Frequency selection

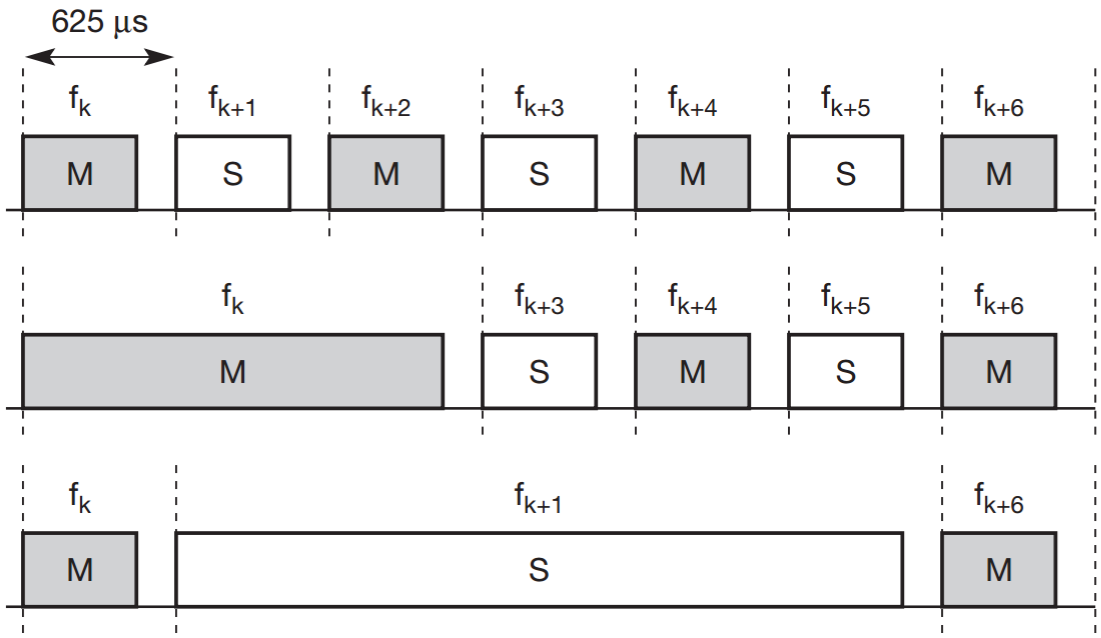


Figure 7.45
Frequency selection during data transmission (1, 3, 5 slot packets)

Baseband Layer

- Packet format
  - 3-bit active Member address for 7 slaves.
  - Payload maximum 343 bytes.

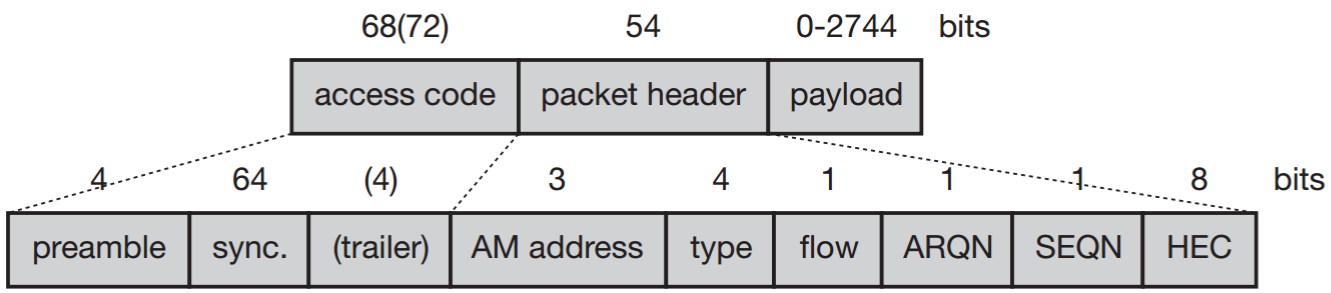


Figure 7.46
Baseband packet format

Baseband Layer

- Physical Links
  - **Synchronous connection-oriented link (SCO):** Classical telephone (voice) connections require symmetrical, circuit-switched, point-to-point connections. For this type of link, the master reserves two consecutive slots (forward and return slots) at fixed intervals.

Baseband Layer

- Physical Links
  - **Asynchronous connectionless link (ACL):** Typical data applications require symmetrical or asymmetrical (e.g., web traffic), packet-switched, point-to-multipoint transfer scenarios (including broadcast). Here the master uses a polling scheme. A slave may only answer if it has been addressed in the preceding slot.

Data Transmission Example

- SCO is allocated every 6 slots.

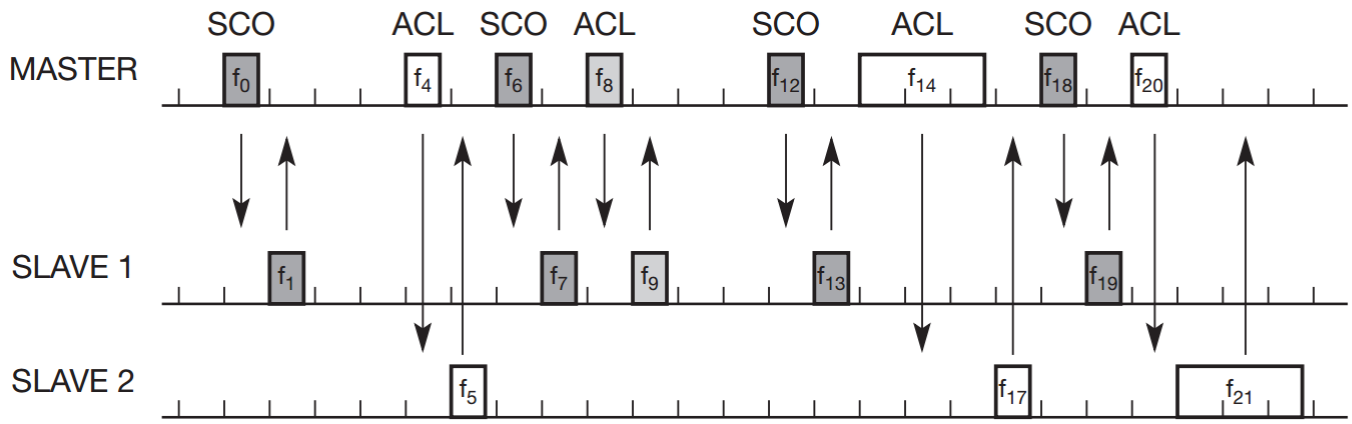


Figure 7.49 Example data transmission

Error Recovery Example

- ARQ: each packet is acknowledged in the next following packet.

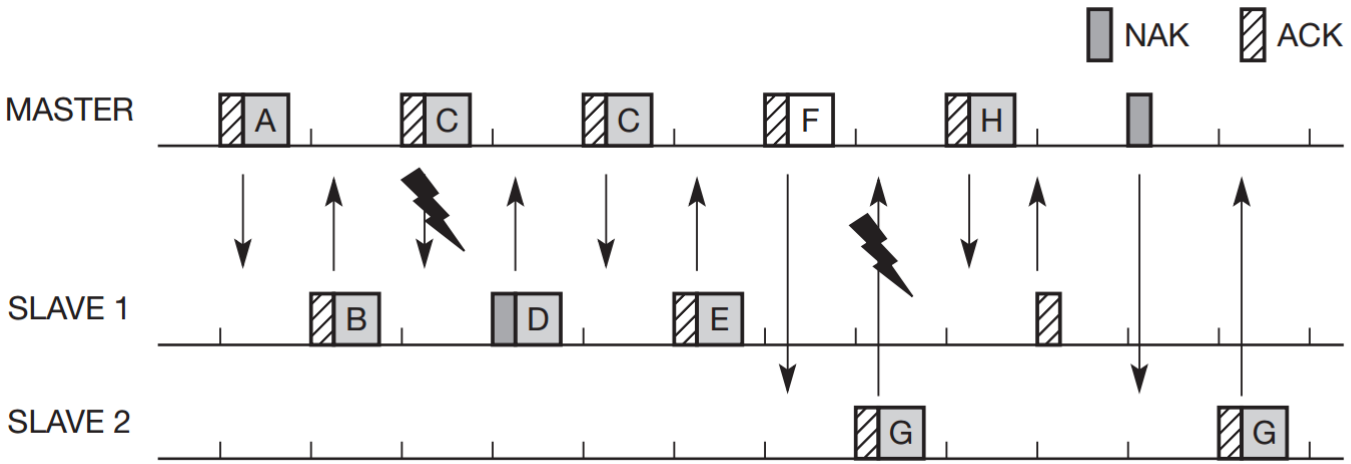
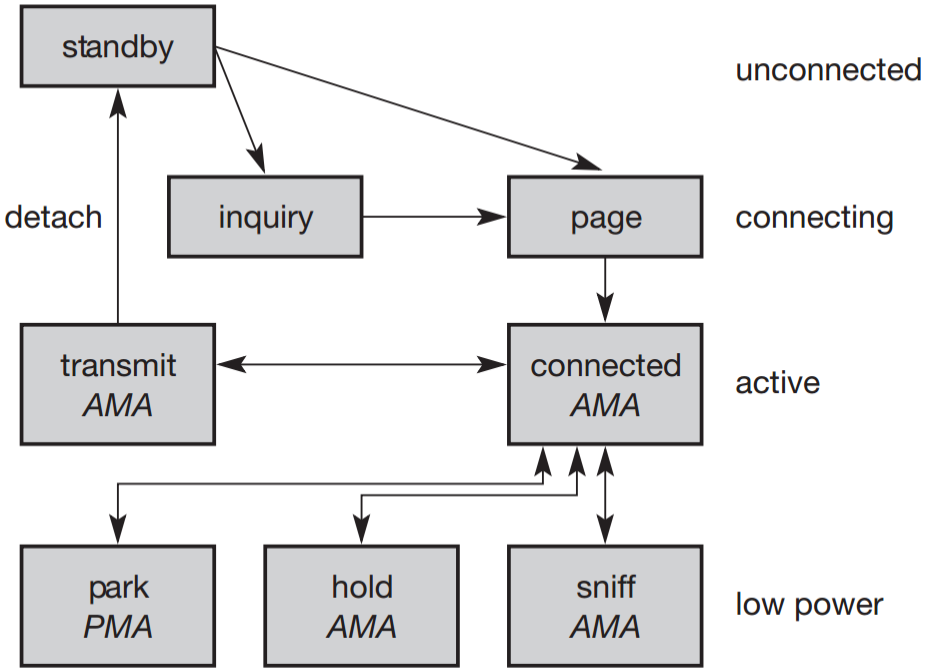


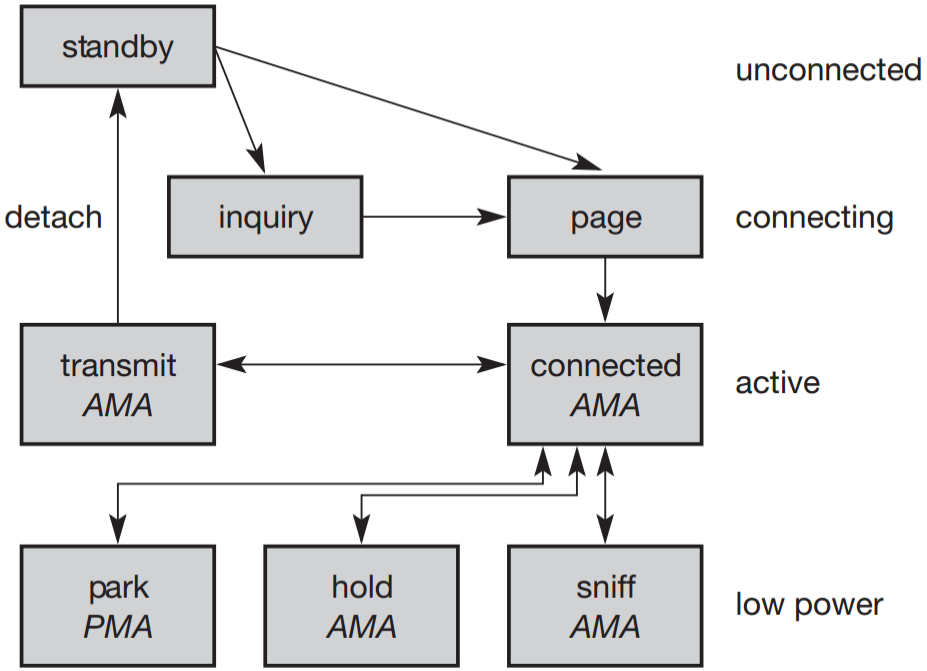
Figure 7.50
Error recovery

Link Manager Protocol



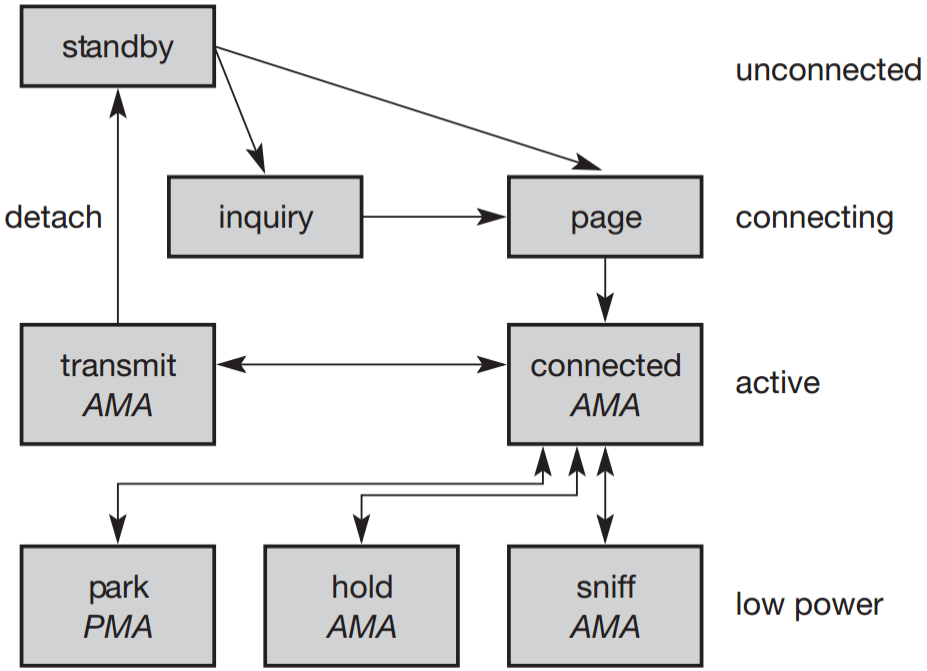
- Standby: device that is currently not participating in a piconet. It is a low power mode where only native clock is running.

Link Manager Protocol



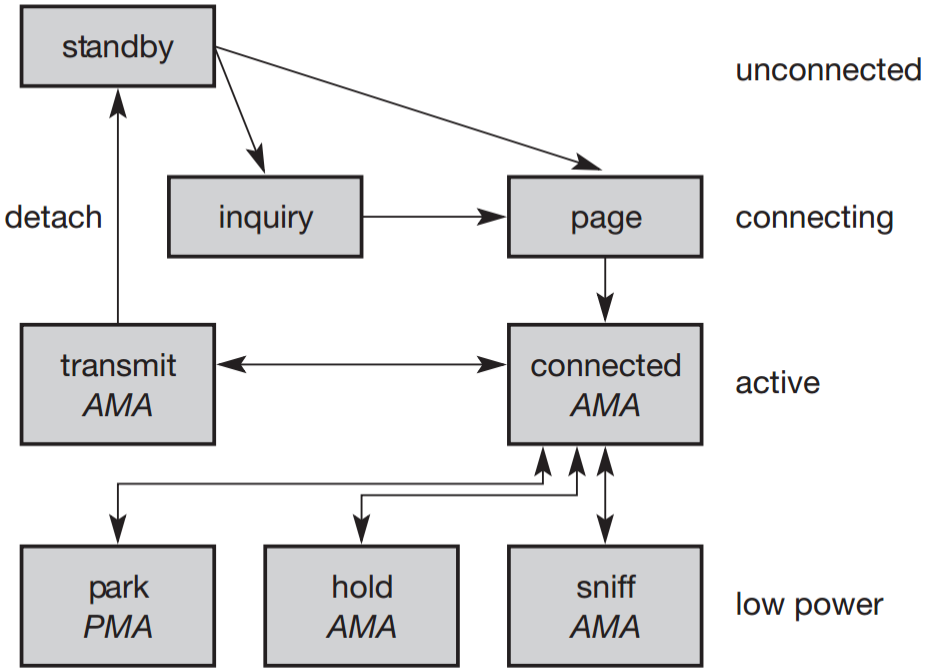
- Inquiry: device want to establish a piconet, or want to listen to the channel.
  - To establish: send out a Inquiry Access Code (IAC).
  - To listen: listen IAC, and join as a slave once receive such code.
  - Inquiry can collide.

Link Manager Protocol



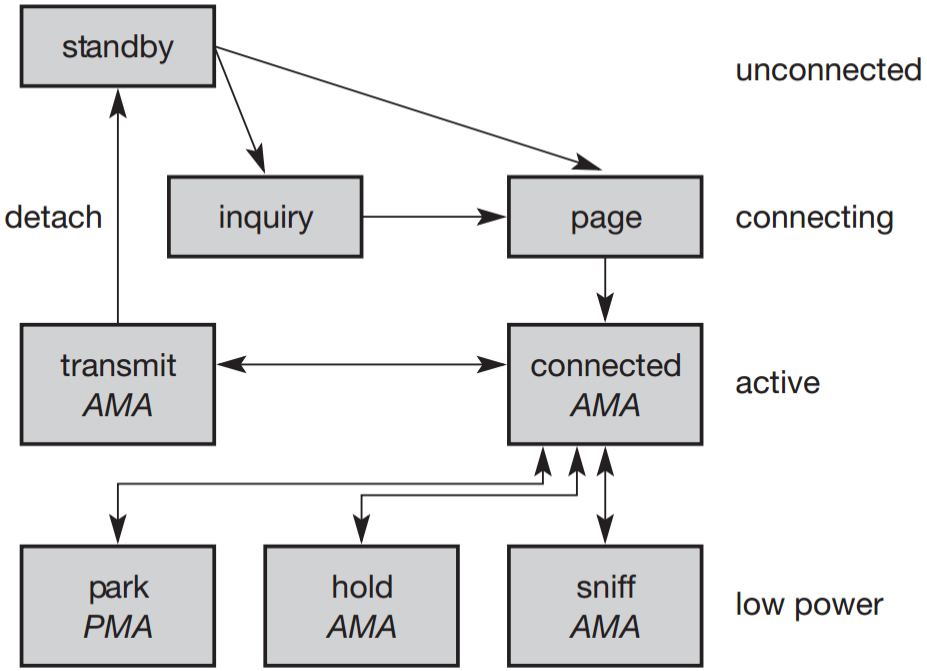
- Master calculates hopping sequences and page slaves.
- Slaves synchronize with master and start connection.

Link Manager Protocol



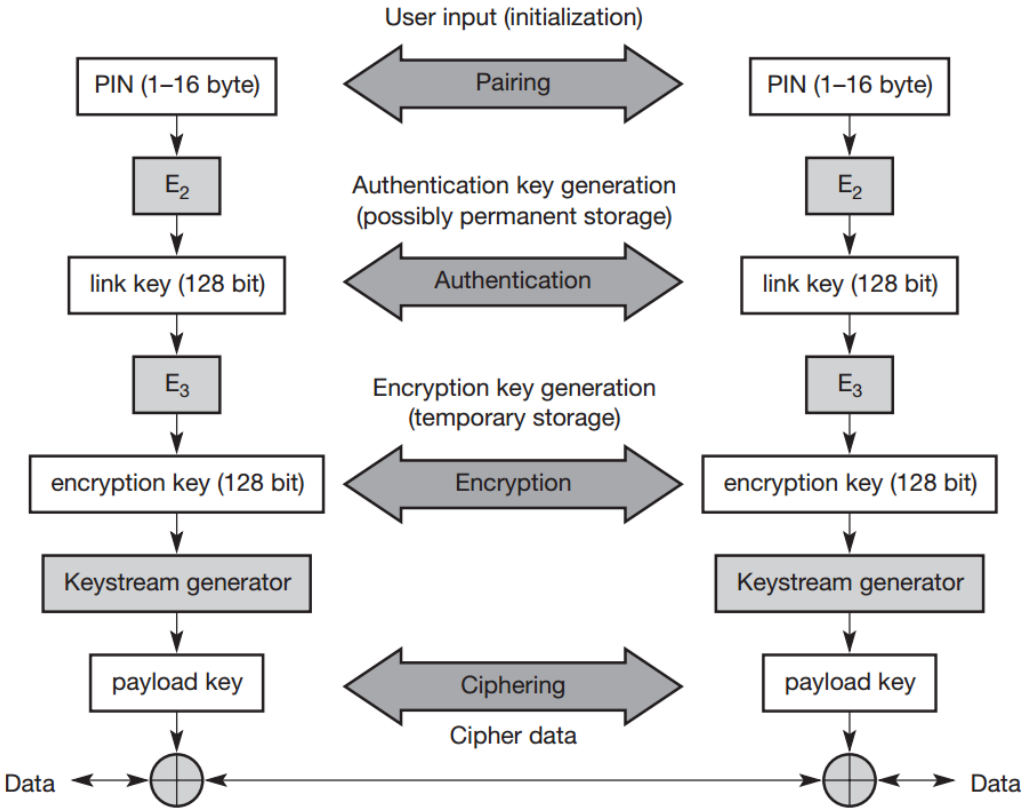
- During connection:
  - Active slaves listen, transmit, and receive.
  - Master periodically sync with slaves.
  - Active member as 3-bit active member address.

Link Manager Protocol



- Sniff: slaves reduce the rate to listen to the piconet, while still keeps active member address.
- Hold: slave stops ACL transmission but keeps its AMA, can have SCO packets.
- Park: slave releases AMA and receives a parked member address. Still sync with master

Security


User input (initialization)
PIN (1–16 byte)
Pairing
PIN (1–16 byte)
E2
Authentication key generation
(possibly permanent storage)
E2
link key (128 bit)
Authentication
link key (128 bit)
E3
Encryption key generation
(temporary storage)
E3
encryption key (128 bit)
Encryption
encryption key (128 bit)
Keystream generator
Keystream generator
payload key
Ciphering
Cipher data
payload key
Data
Data