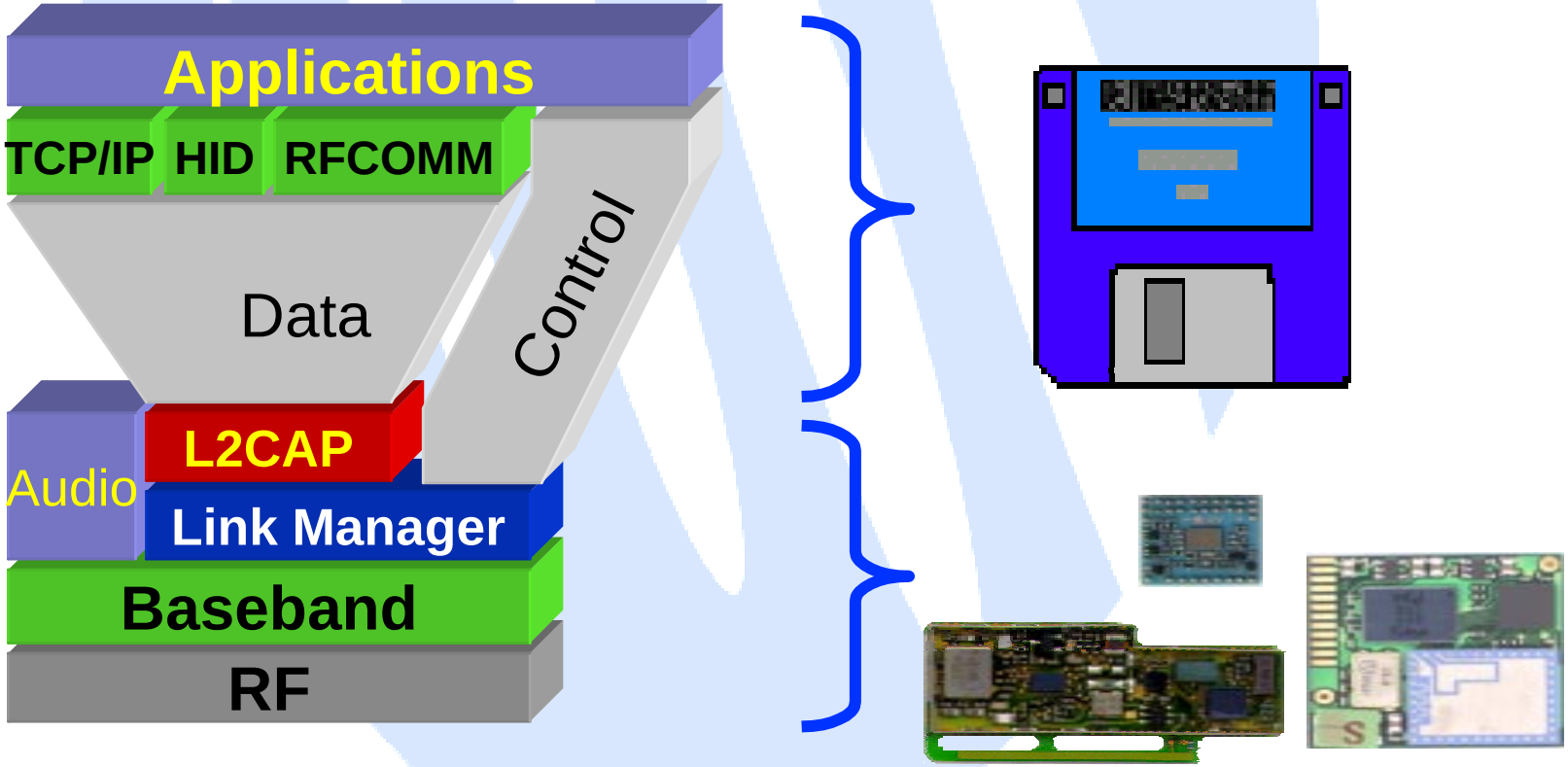
Hardware architecture overview

Dr. Jaap Haartsen

Ericsson Radio Systems
jaap.haartsen@erh.ericsson.se

WHAT IS BLUETOOTH?



- a hardware description
- an application framework

OUTLINE

- **Air interface**
  - Radio
  - Baseband
- **Hardware implementation**

RADIO

RADIO PARAMETERS (1)

- **Frequency hopping**
  - ISM band at 2.45 GHz
  - 2402 + *k* MHz, *k* = 0, …, 78
  - device-specific hopping sequence
  - nominal rate 1600 hops/s
- **Modulation**
  - binary FSK
  - Gaussian shaping
  - BT = 0.5; 0.28 < *h* < 0.35
  - -20dB bandwidth of 1 MHz

RADIO PARAMETERS (2)

- **Transmit power**
  - nominal 0 dBm
  - up to 20 dBm provided power control
- **Receiver sensitivity**
  - -70 dBm @ 0.1% BER

2.4 GHz ISM BAND

Restrictions

- Spectrum spreading must be employed
- Channel bandwidth limited to 1 MHz
- Multiple uncoordinated networks may exist and cause interference
- Microwave ovens also use this band
- 2.4 GHz IC electronics must run at high current levels

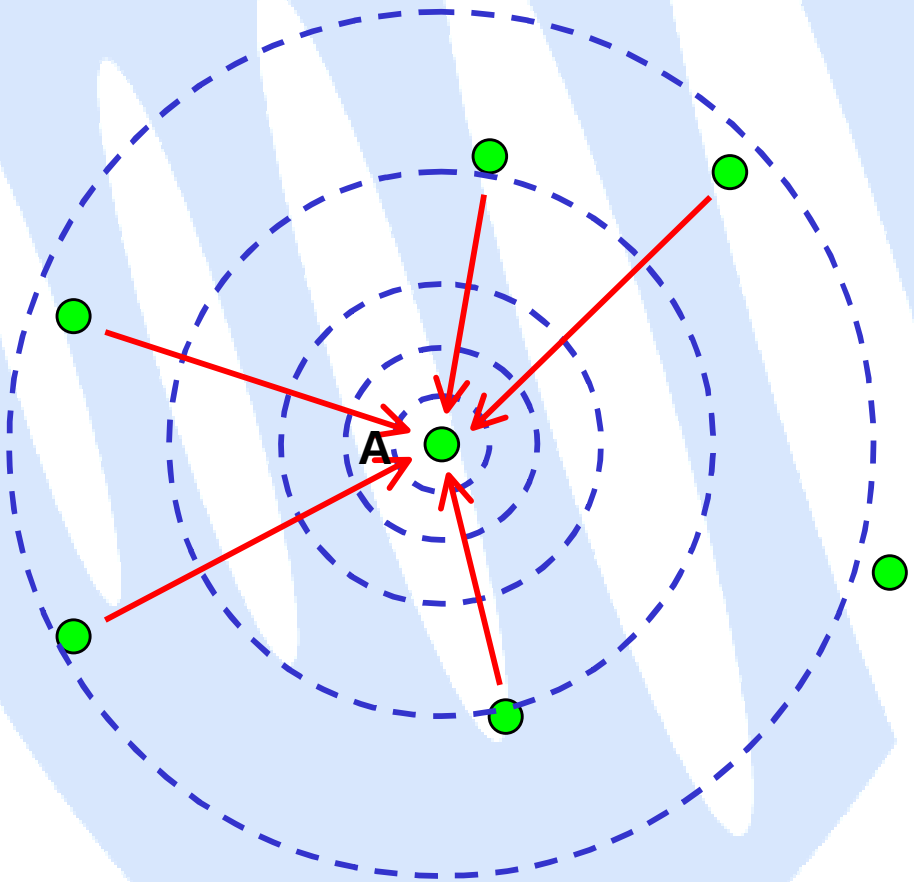
Bluetooth solution

- Frequency hop spread spectrum
- 1 Mb/s symbol rate exploits maximum channel bandwidth
- Fast frequency hopping and short data packets
- CVSD voice coding enables operation at high bit error rates
- Air interface tailored to minimize current consumption
- Relaxed link budget supports low cost single chip integration

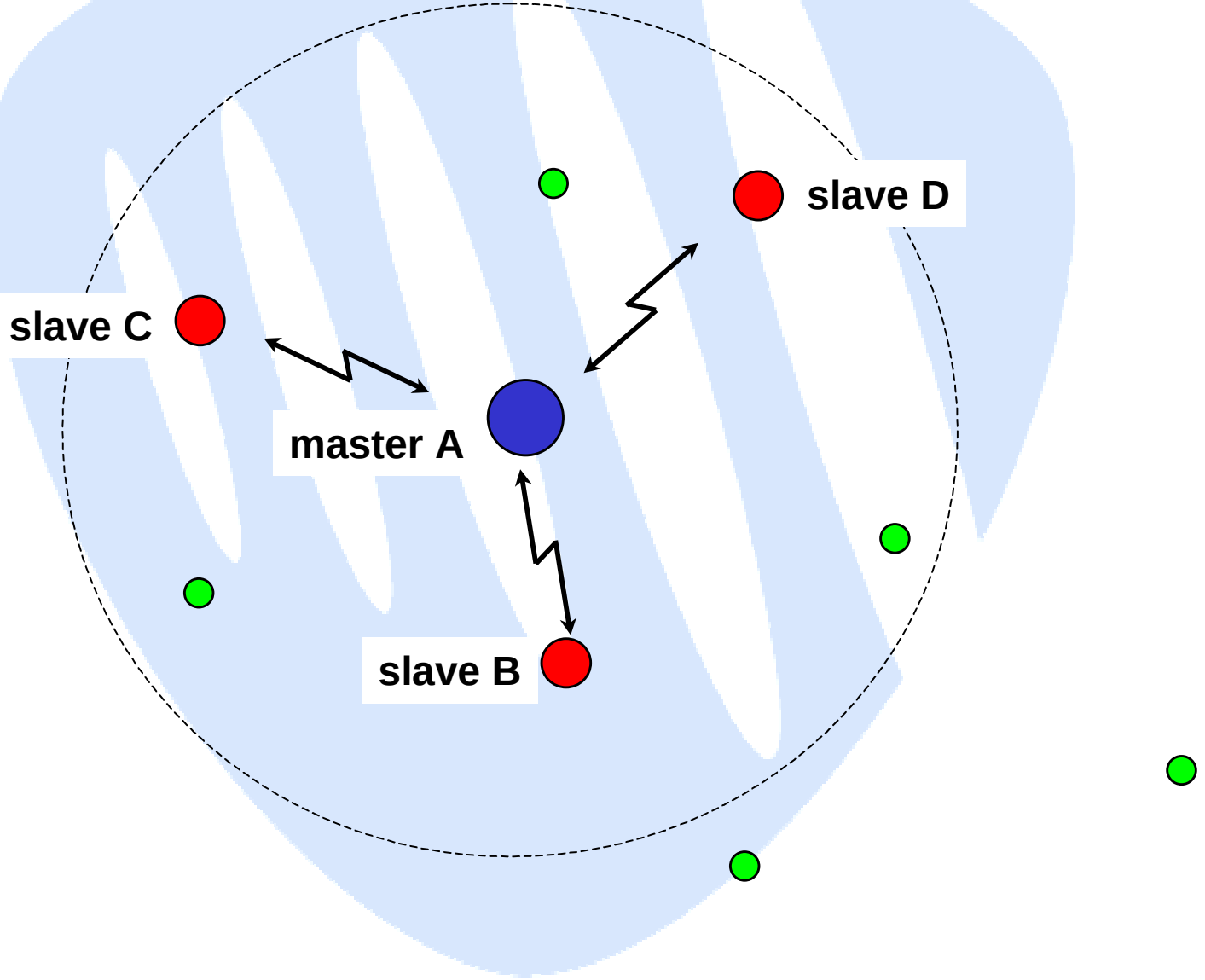
BASEBAND OPERATIONS

CONNECTION ESTABLISHMENT

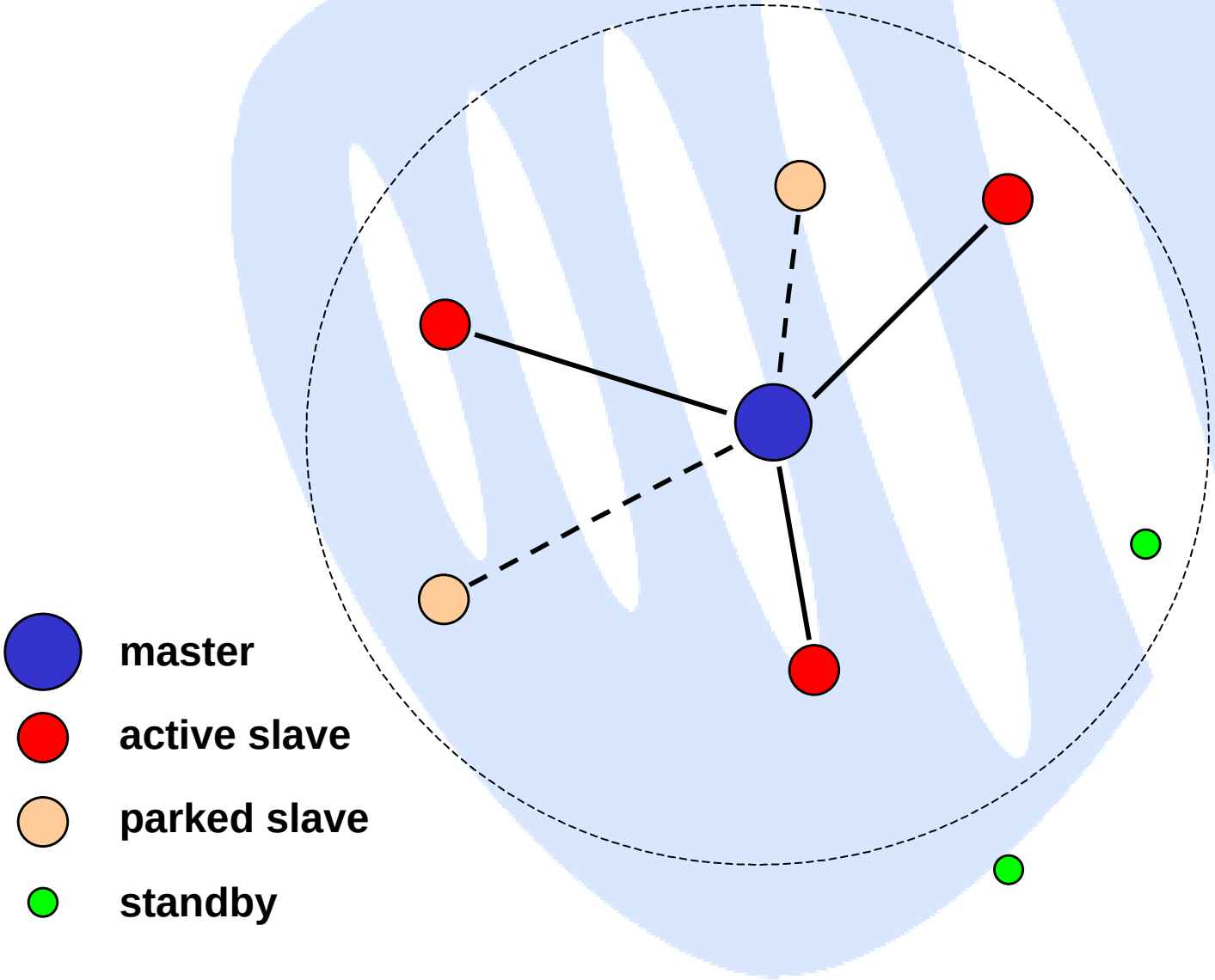
INQUIRY



CREATING A PICONET



OPERATIONAL STATES



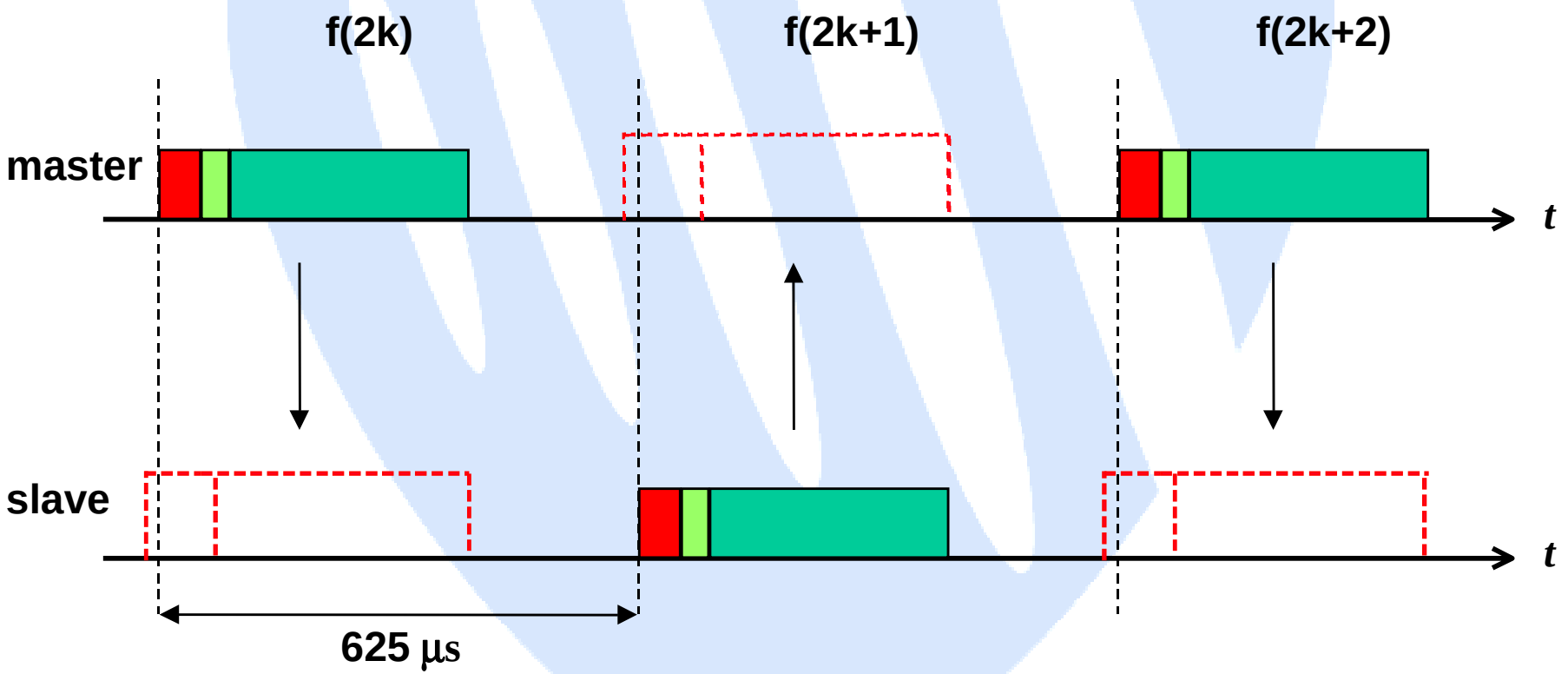
ADDRESSING

- **Bluetooth Device Address** (BD_ADDR)
  - 48-bit IEEE 802 address
  - 24-bit lower address part (LAP)
  - 8-bit upper address part (UAP)
- **Active Member Address** (AM_ADDR)
  - 3-bit active slave address
  - all-zero broadcast address
- **Parked Member Address** (PM_ADDR)
  - 8-bit parked slave address

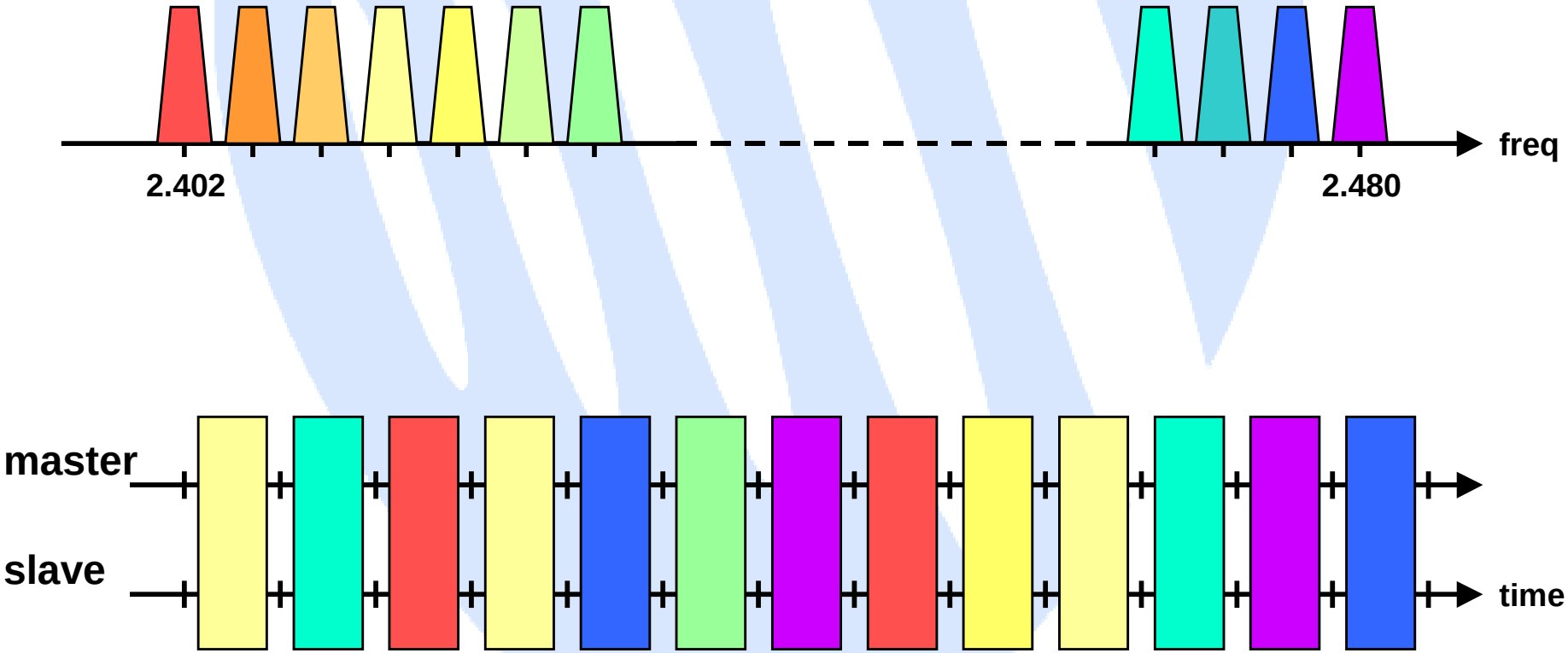
BASEBAND OPERATIONS

PICONET CHANNEL

FH/TDD CHANNEL

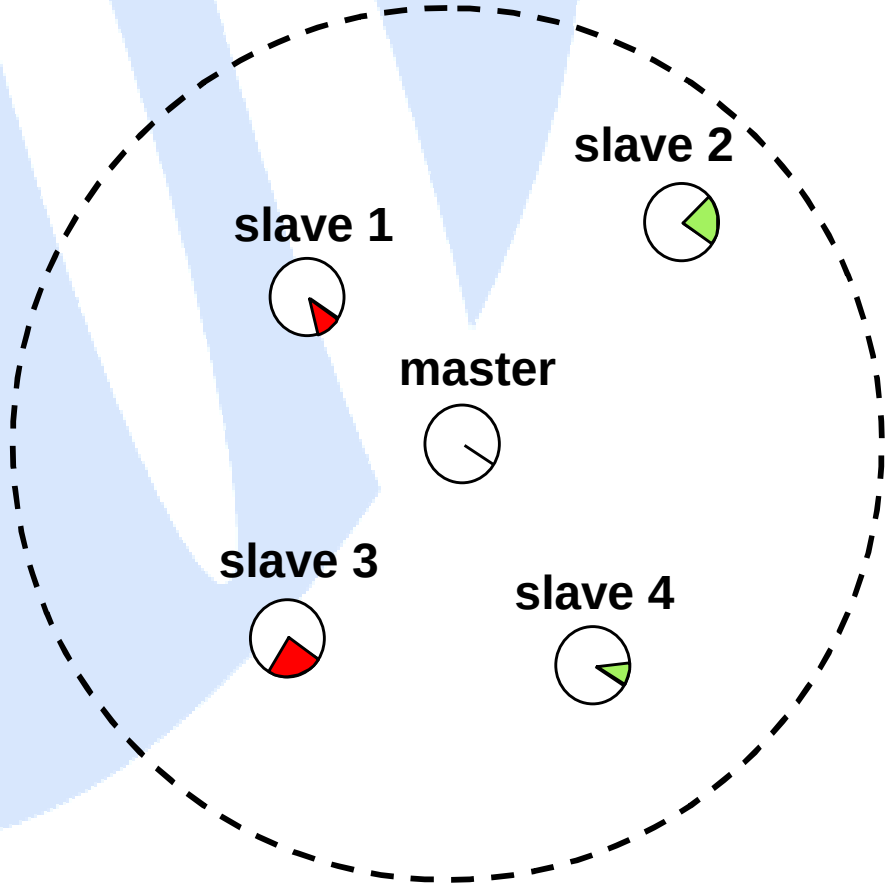


FREQUENCY HOPPING

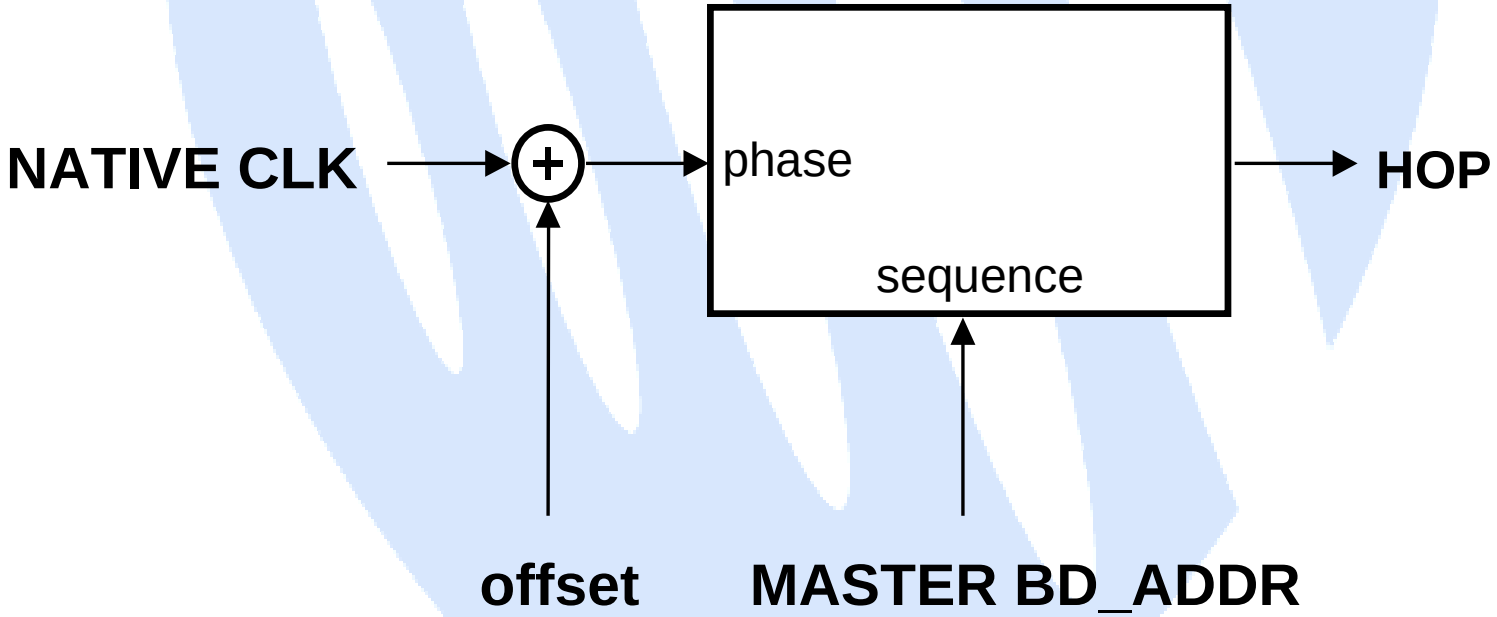


PHYSICAL CHANNEL

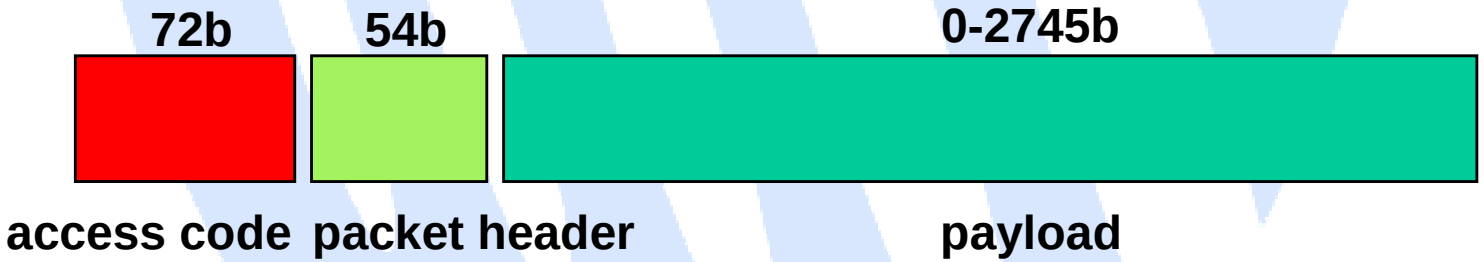
- master BD_ADDR → hop sequence
- master CLOCK → phase



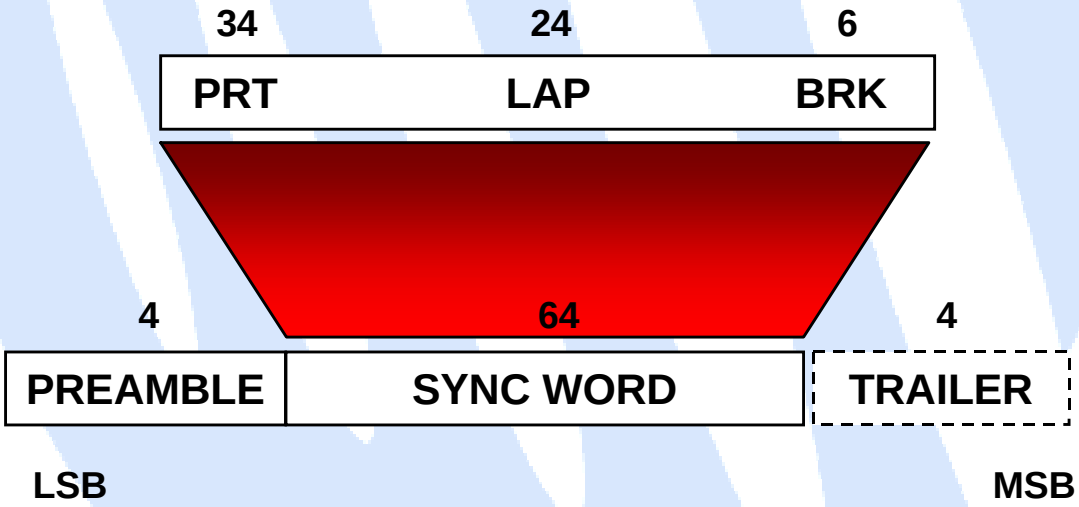
HOP SELECTION



PACKET FORMAT



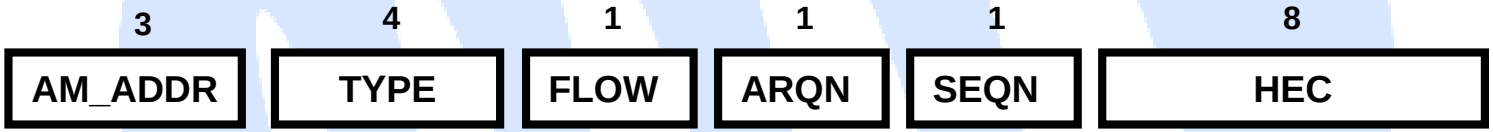
ACCESS CODE



ACCESS CODE TYPES

- **Device access code (DAC)**
  - unit identifier
  - derived from unit LAP
- **Channel access code (CAC)**
  - channel identifier
  - derived from master LAP
- **Inquiry access code (IAC)**
  - reserved identifier
  - derived from reserved address

PACKET HEADER



parameter	information
AM_ADDR	slave active member address
TYPE	payload type
FLOW	LC flow control
ARQN	ACK/NAK
SEQN	retransmit ordering
HEC	header error check

PHYSICAL LINK DEFINITION

Purpose: **MULTI-MEDIA SUPPORT**

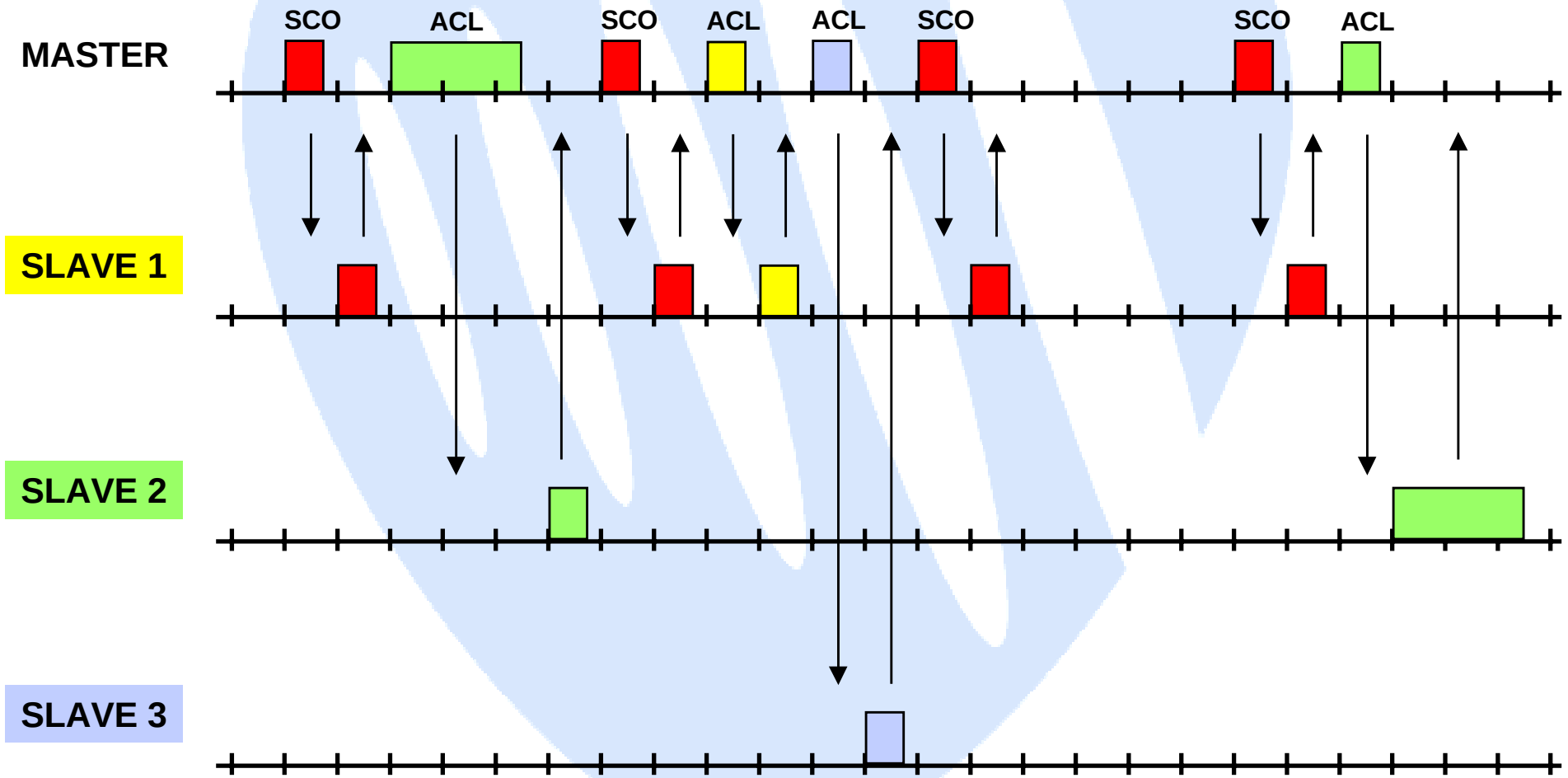
Mixing:

- circuit switching
- packet switching

PHYSICAL LINK TYPES

- **Synchronous Connection-Oriented (SCO) Link**
  - circuit switching
  - symmetric, synchronous services
  - slot reservation at fixed intervals
- **Asynchronous Connection-Less (ACL) Link**
  - packet switching
  - (a)symmetric, asynchronous services
  - polling access scheme

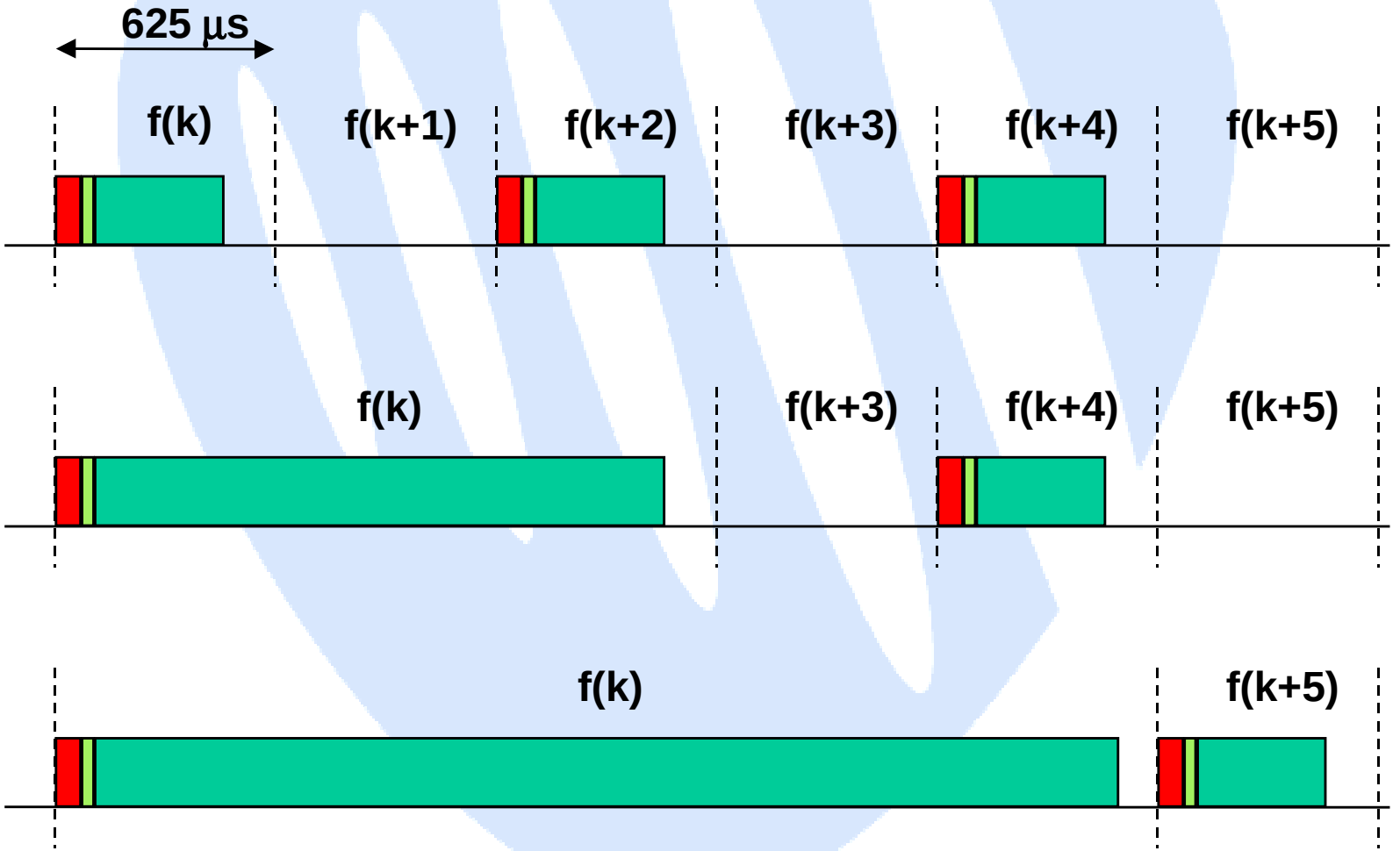
MIXED LINK EXAMPLE



PACKET TYPES

segment	type	SCO link	ACL link
1	0000	NULL	NULL
	0001	POLL	POLL
	0010	FHS	FHS
	0011	DM1	DM1
2	0100		DH1
	0101	HV1	
	0110	HV2	
	0111	HV3	
	1000	DV	
	1001		AUX1
3	1010		DM3
	1011		DH3
	1100		
	1101		
4	1110		DM5
	1111		DH5

MULTI-SLOT PACKETS



DATA RATES (kb/s)

type	symmetric	asymmetric	
DM1	108.8	108.8	108.8
DH1	172.8	172.8	172.8
DM3	258.1	387.2	54.4
DH3	390.4	585.6	86.4
DM5	286.7	477.8	36.3
DH5	433.9	723.2	57.6

LINK CONTROL PACKETS

- ID packet
- NULL packet
- POLL packet
- FHS packet

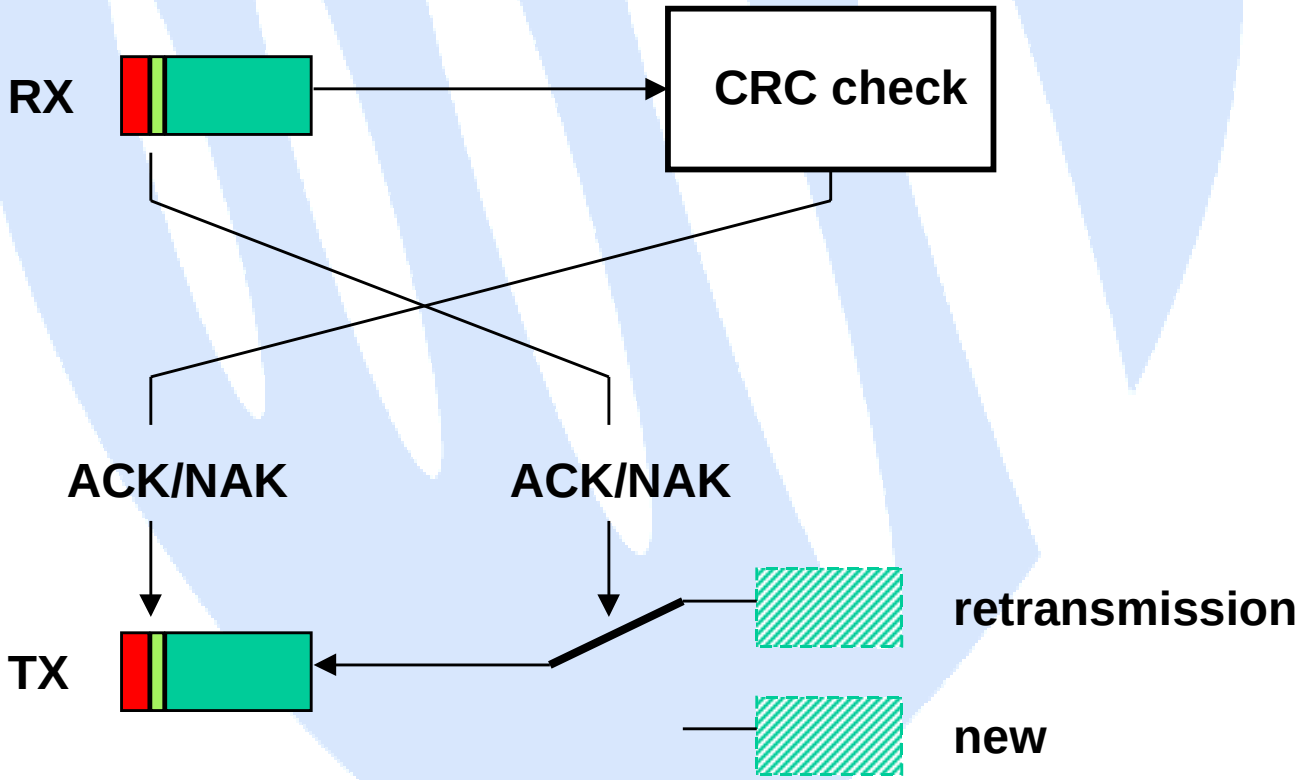
FHS PACKET

- BD_ADDR
- DAC
- AM_ADDR
- class of device
- paging class
- real-time clock

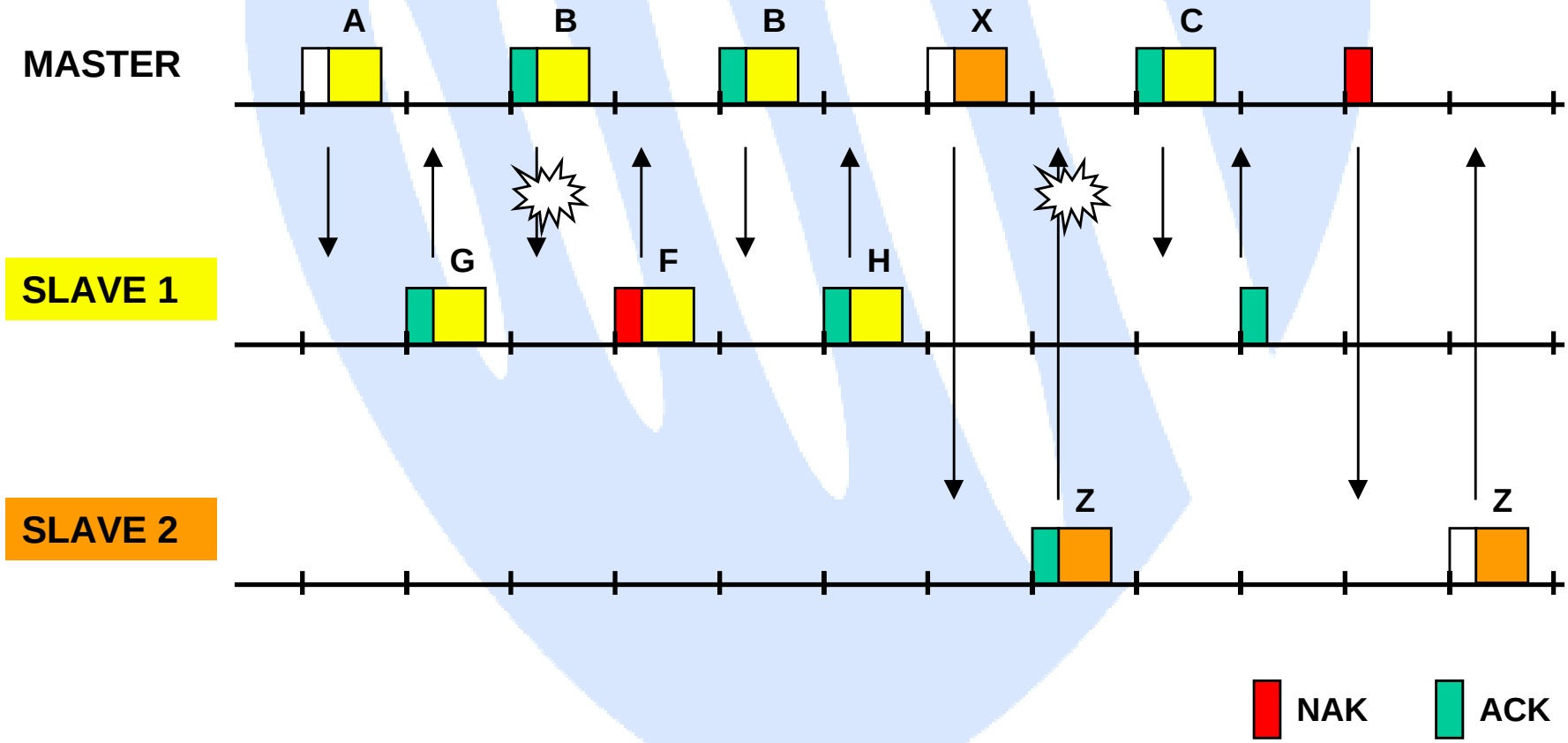
ERROR CORRECTION

- **Forward-Error Correction** (FEC)
  - 1/3 rate: bit-repeat code
  - 2/3 rate: (15,10) shortened Hamming code
- **Automatic Retransmission Query** (ARQ)
  - 1-bit fast ACK/NAK
  - 1-bit sequence number
  - header piggy-backing

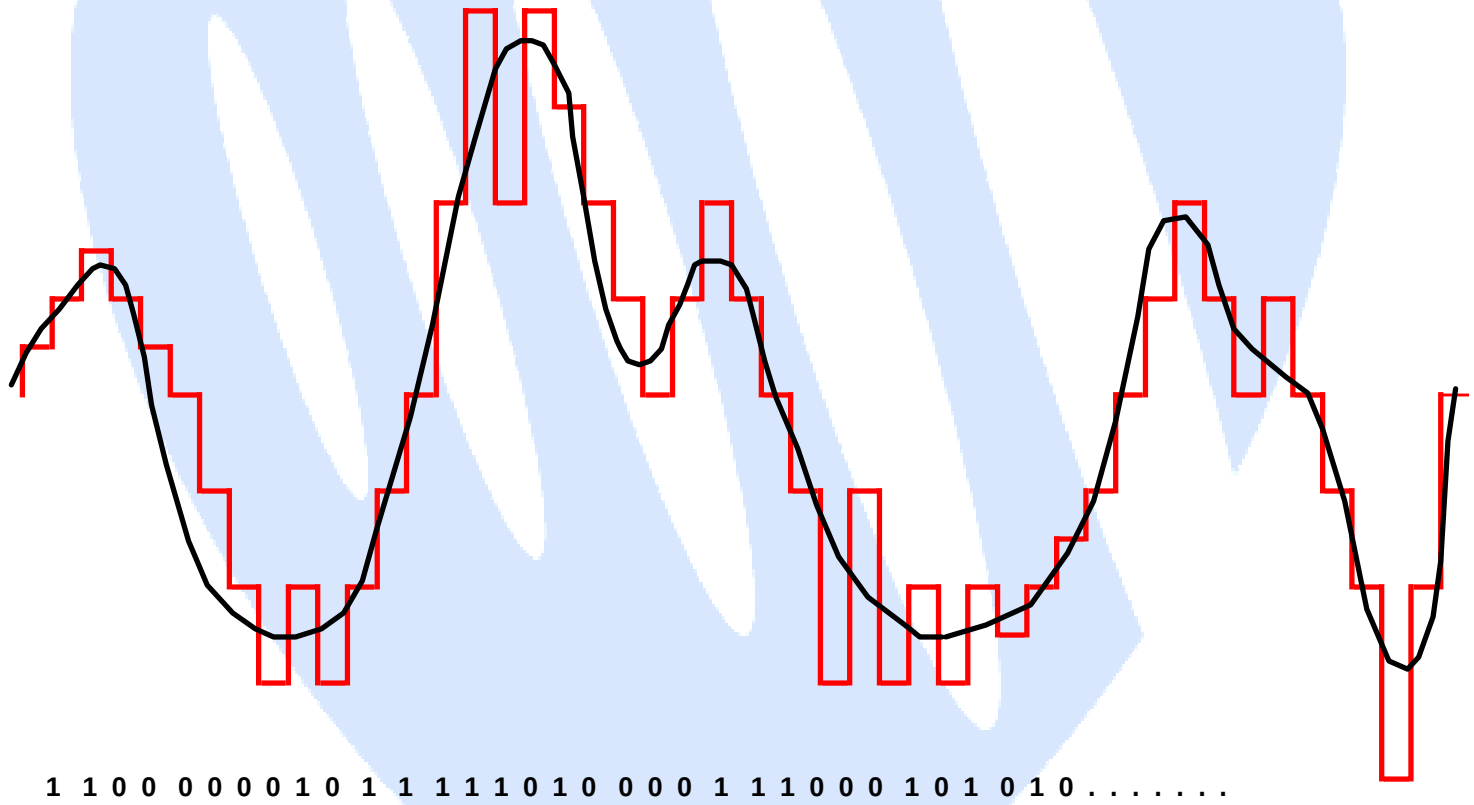
ARQ OPERATIONS



AUTOMATIC RETRANSMISSION



CVSD WAVEFORM CODING



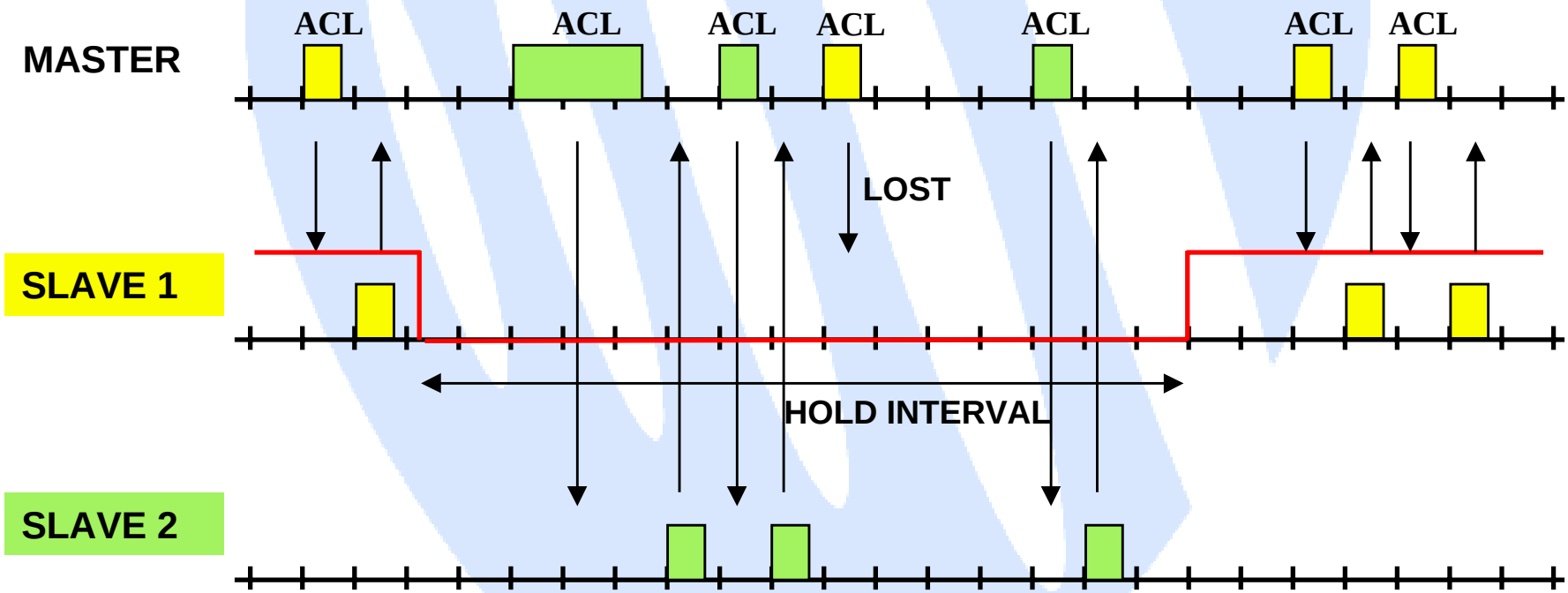
BASEBAND OPERATIONS

PICONET MANAGEMENT

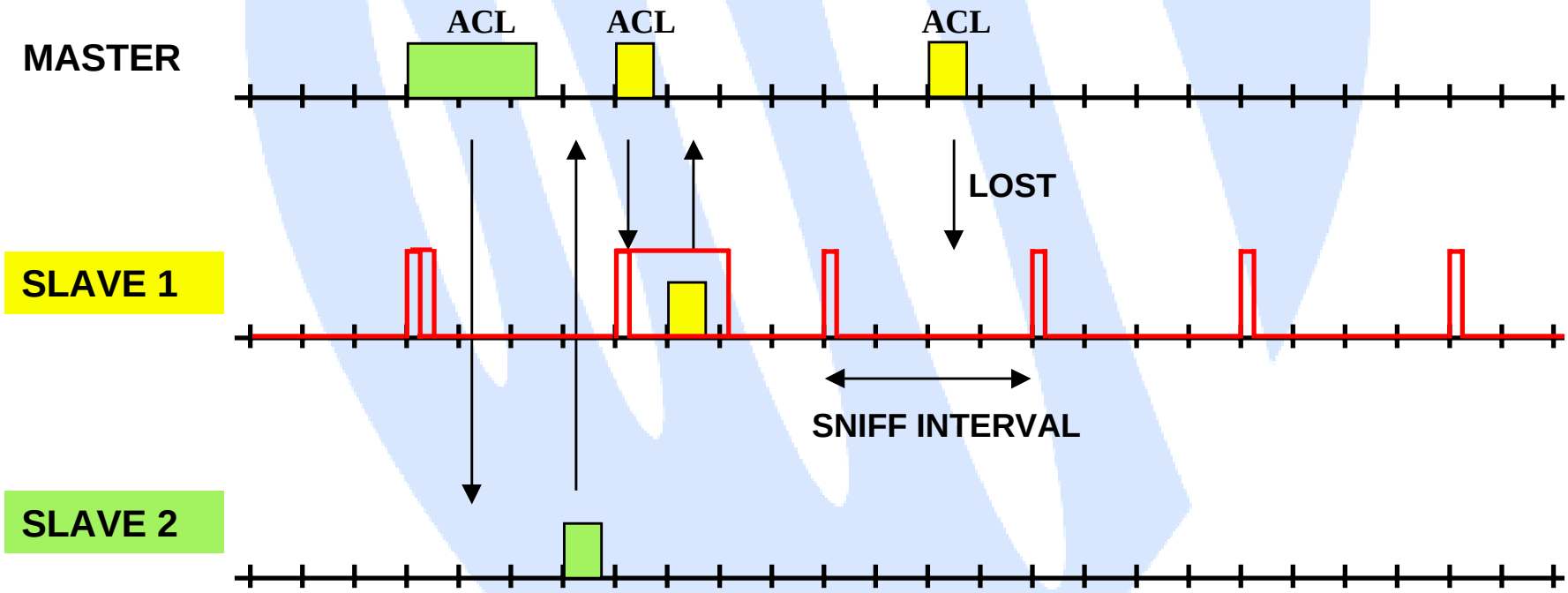
OPERATIONAL STATES

- **stand-by, scan**
- **page, inquiry**
- **connection**
  - active
  - hold
  - sniff
  - park

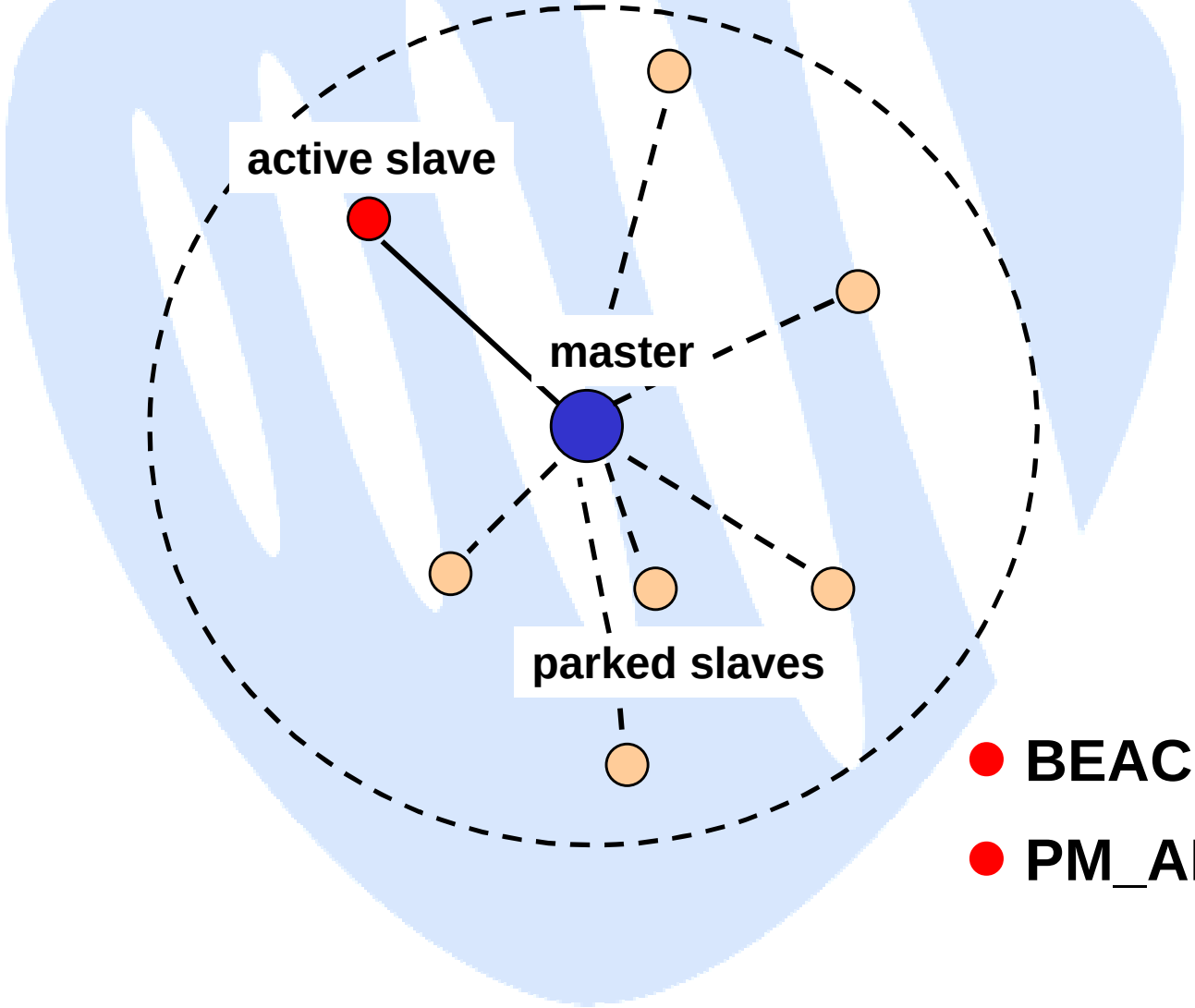
HOLD MODE


MASTER
ACL
ACL
ACL
ACL
ACL
ACL
ACL
LOST
SLAVE 1
HOLD INTERVAL
SLAVE 2

SNIFF MODE

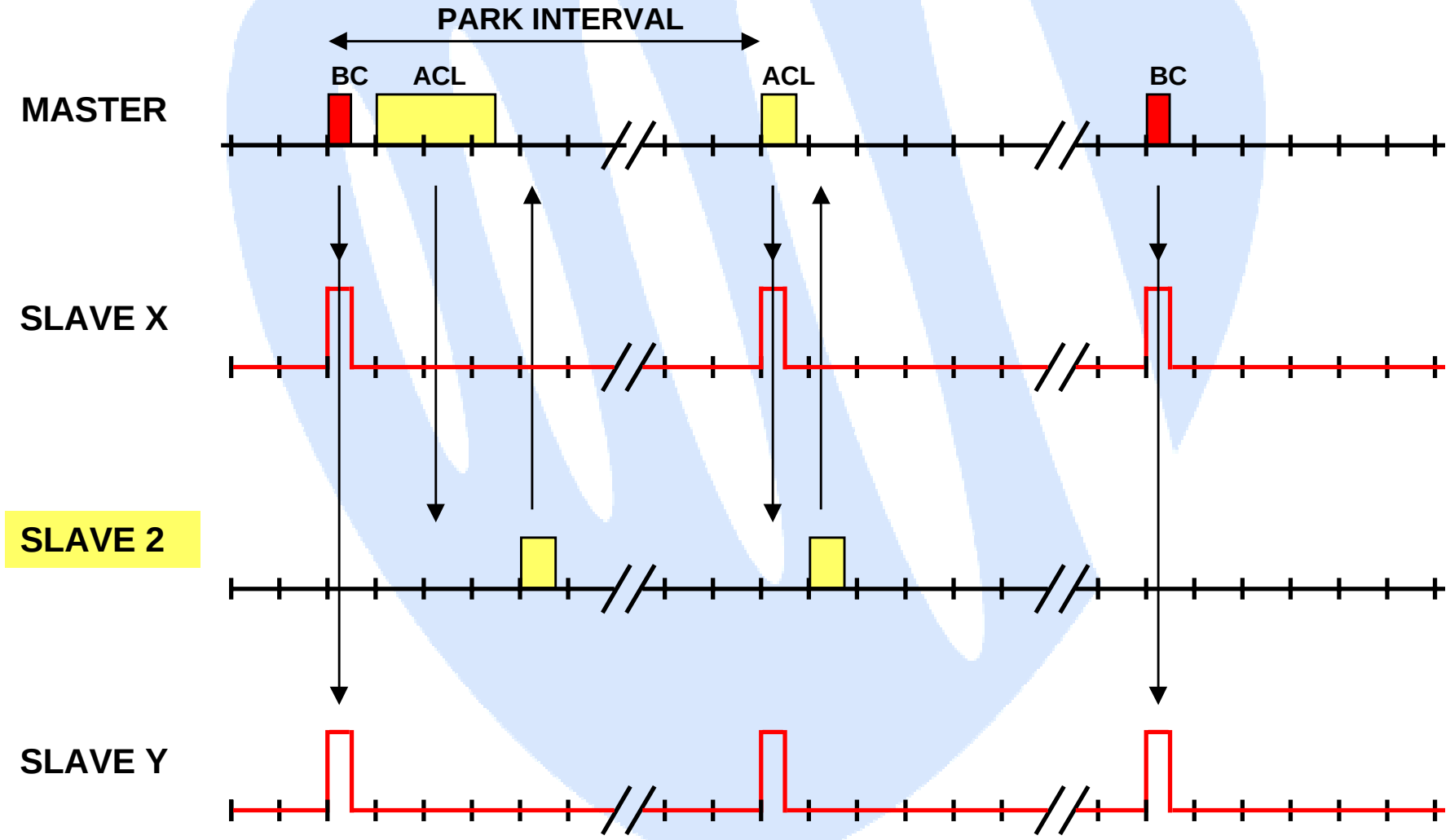


PARK MODE

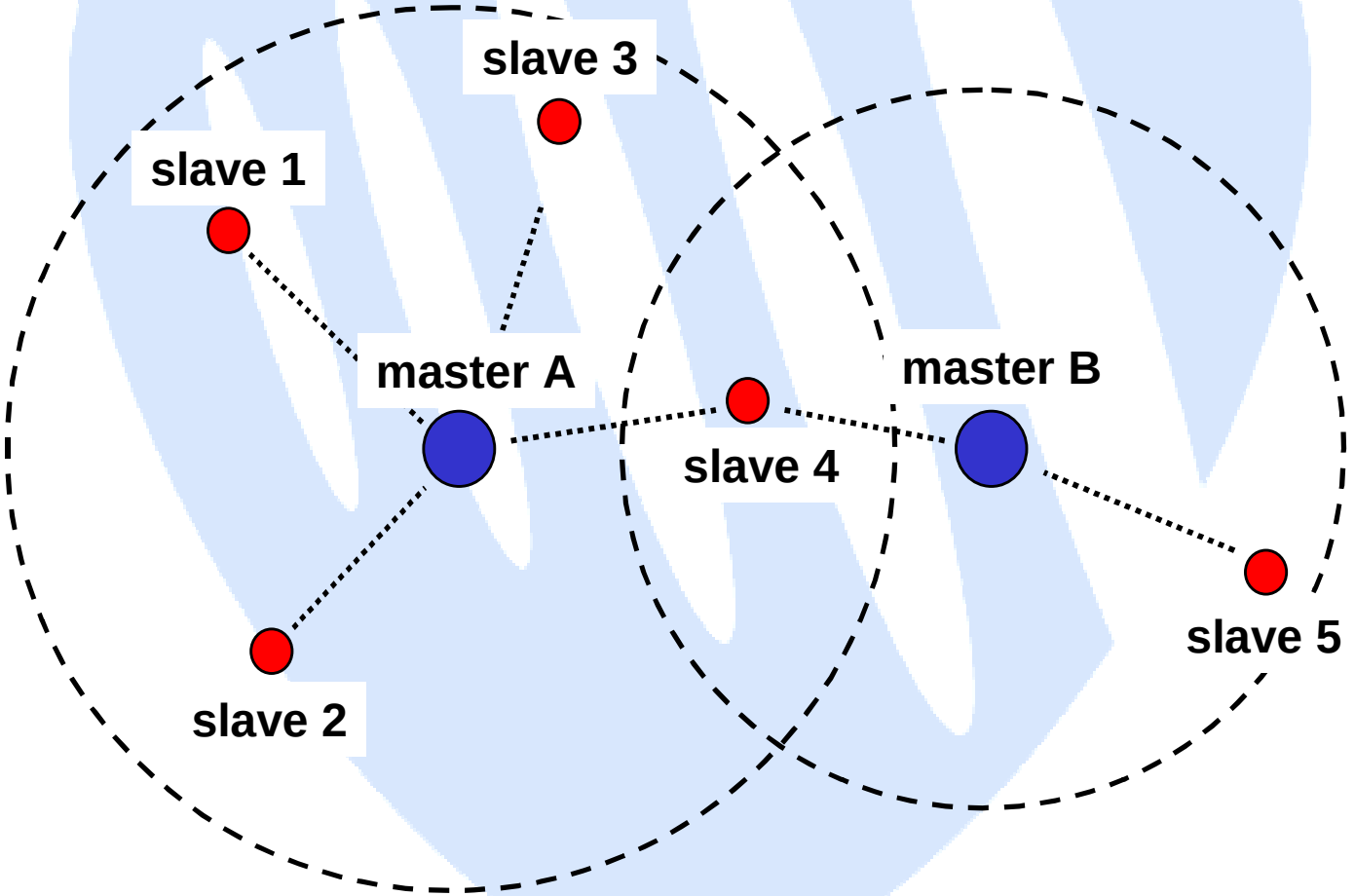


- BEACON
- PM_ADDR

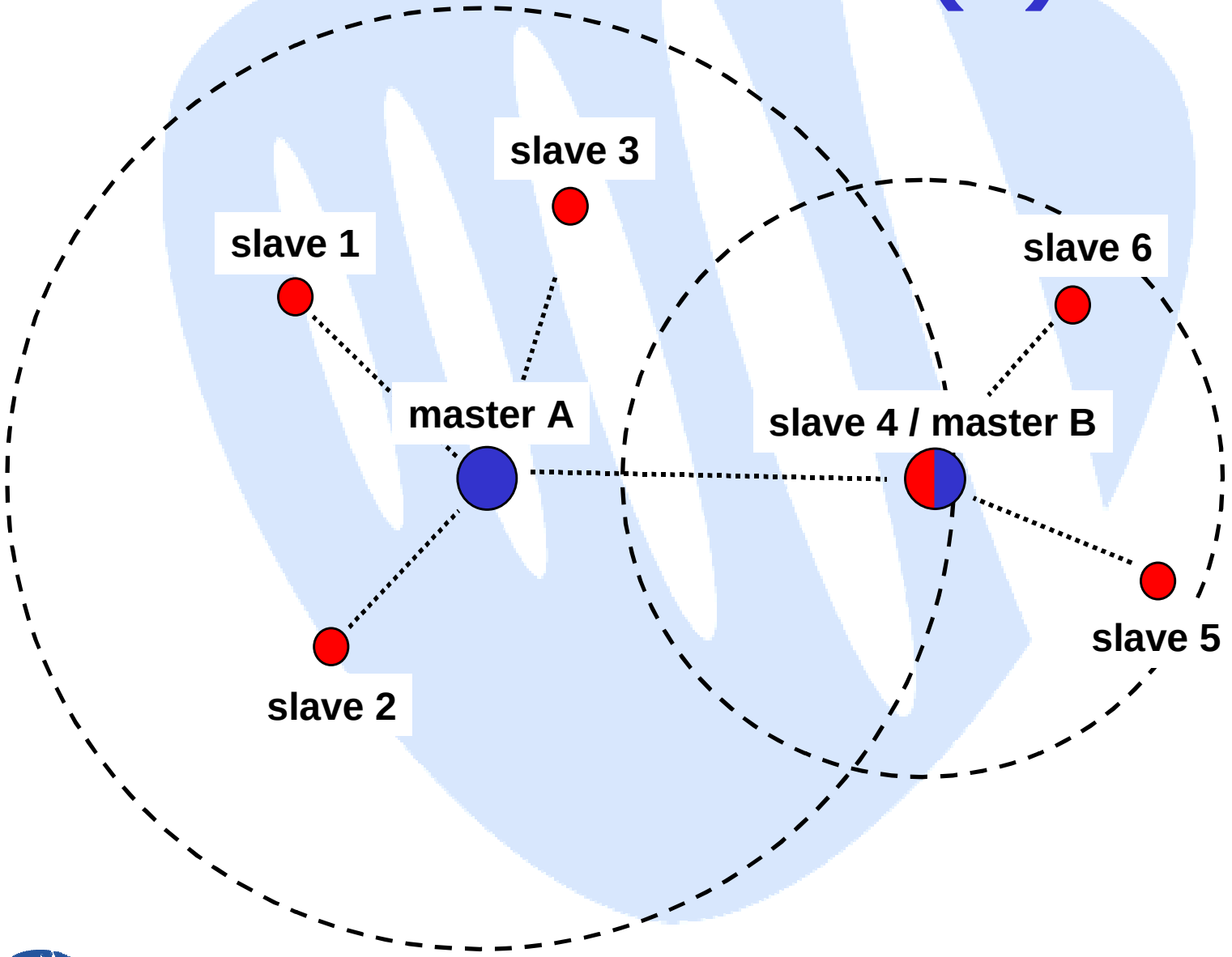
PARK MODE



SCATTERNET (1)



SCATTERNET (2)



BASEBAND OPERATIONS

SECURITY

SECURITY COMPONENTS

- Authentication
- Payload encryption
- Key handling

AUTHENTICATION

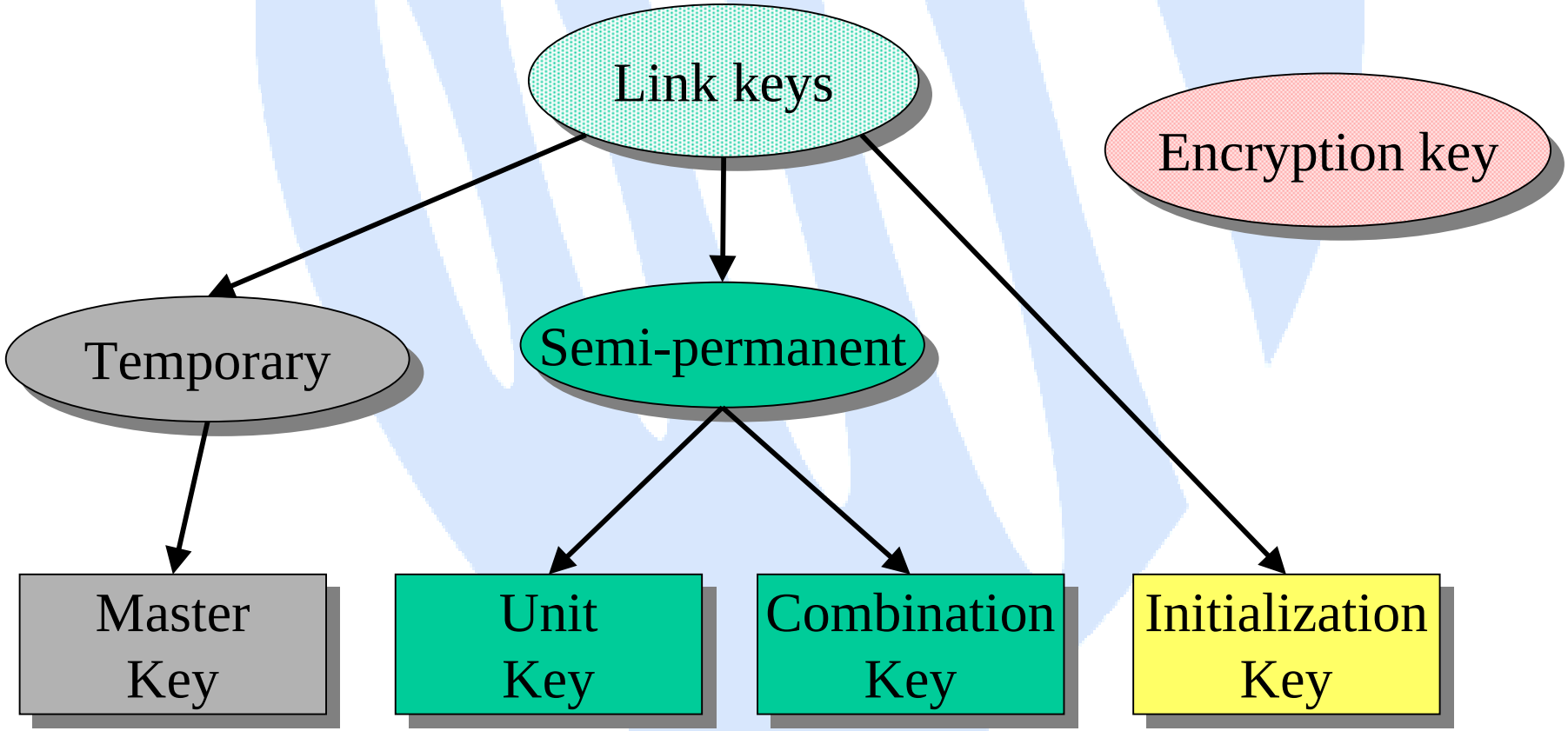
- **To verify claimed identity**
- **Challenge-response system**
- **Algorithm E_1:**
  - Input: RAND (128 bit), Claimant addr. (48 bit), link key (128)
  - Output: *SRES* (32 bit), *ACO* (96 bit)
- **One-sided or mutual authentication**

ACO = Authenticated Ciphering Offset

ENCRYPTION

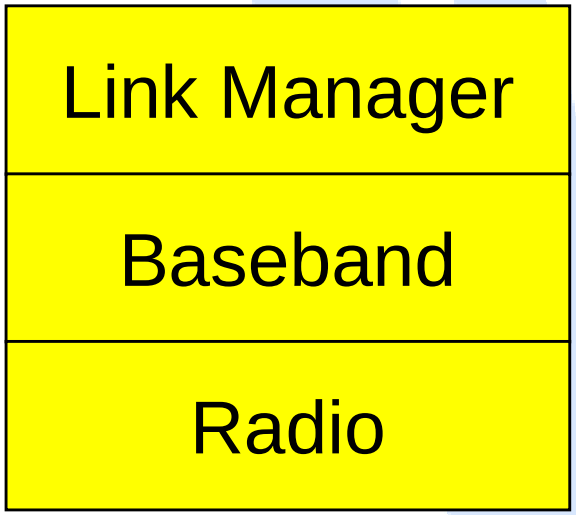
- **To prevent (un)intentional eavesdropping**
- **Stream ciphering**
- **Algorithm E_0:**
  - Input: RAND (128 bit), master addr./clock, K_c (128 bit)
  - Output: cipher stream
- **LFSR restart for every slot**
- **Encrytion of payload only**
- **Point-to-point or point-to-multipoint**

KEY TYPES


Link keys
Encryption key
Temporary
Semi-permanent
Master Key
Unit Key
Combination Key
Initialization Key

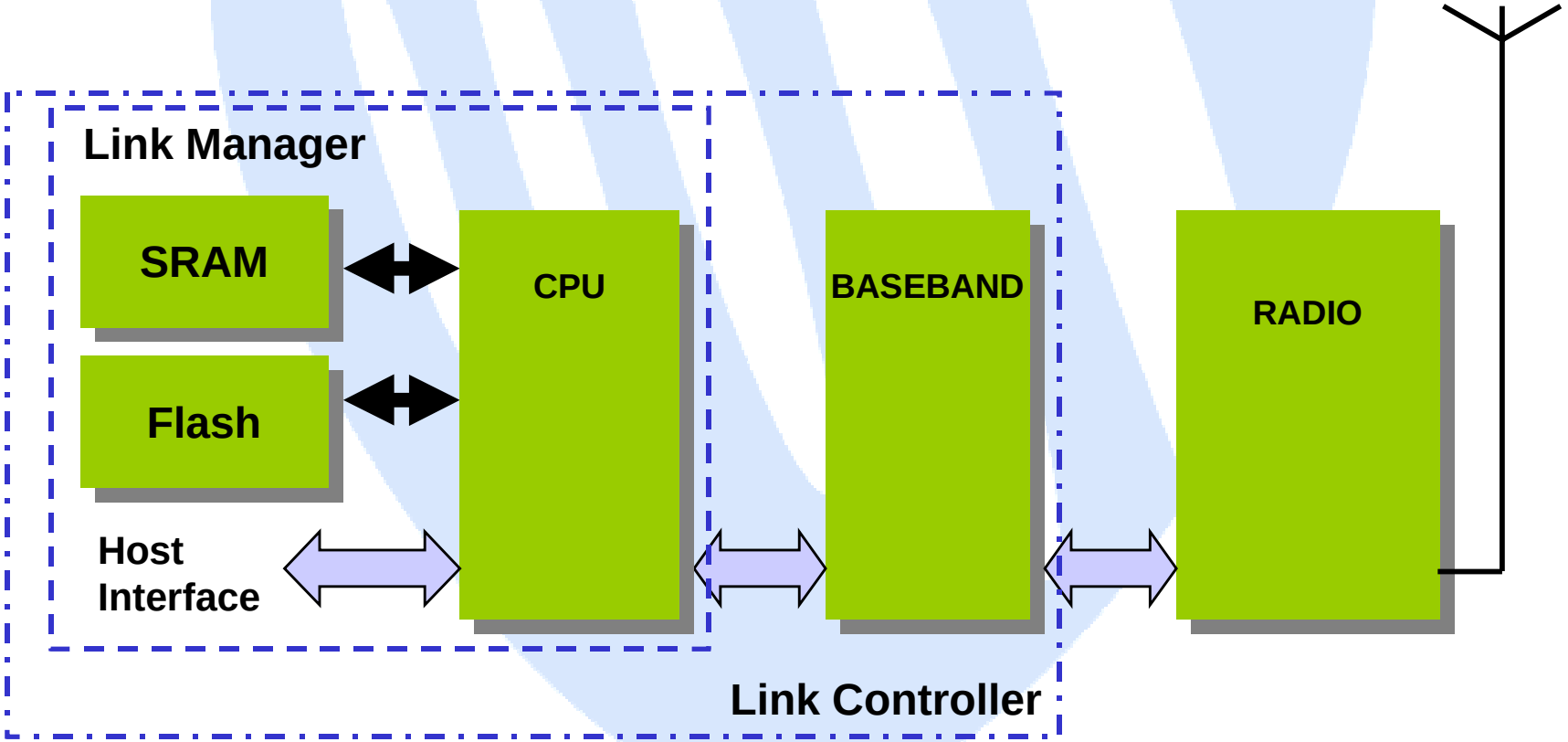
IMPLEMENTATION

LAYERED CONCEPT



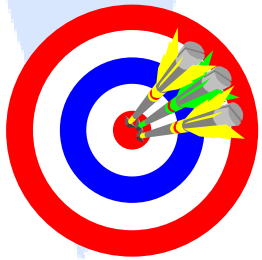
- **LINK MANAGER**
  - connection establishment/release
  - link handling
- **BASEBAND CONTROLLER**
  - coding / ciphering
  - packet handling
  - frequency hopping
- **RADIO**
  - frequency synthesis
  - conversion bits into symbols
  - filtering

FUNCTIONAL PARTITIONING

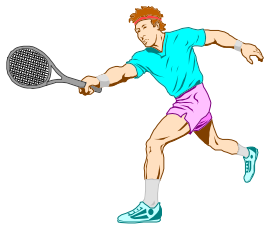


"Design a radio to replace the cable and its connectors..."

- **Design goals**
  - small implementation size
  - low implementation cost
  - low power consumption
  - secure and robust for open ISM band

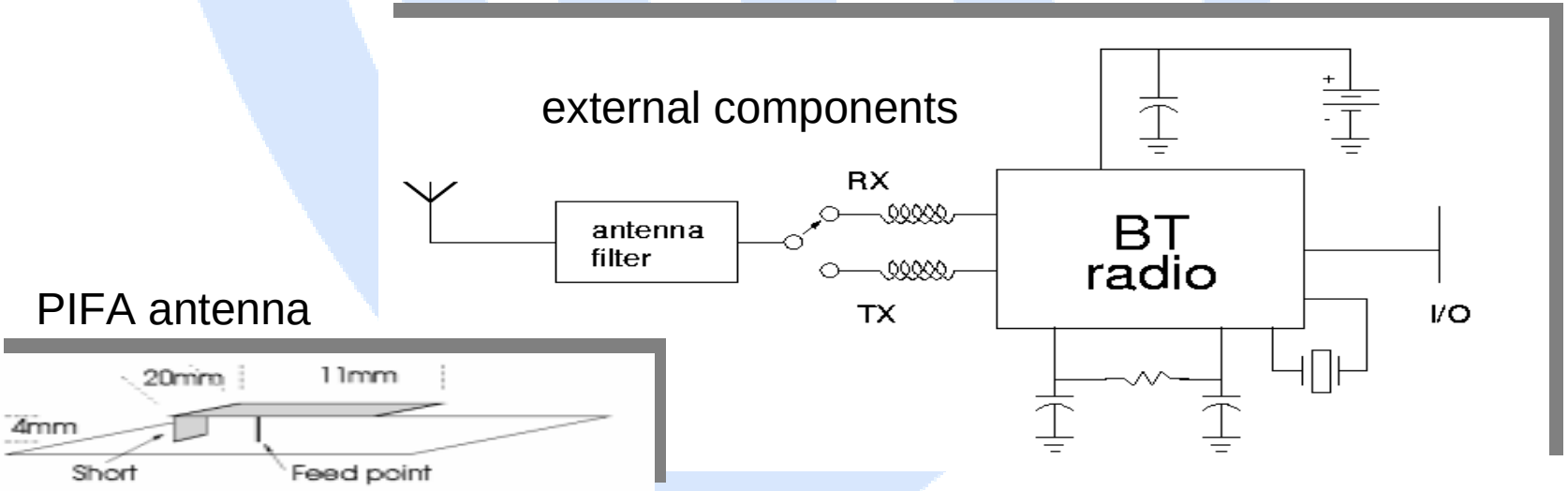


- **Challenges**
  - fast frequency hopping
  - single chip integration



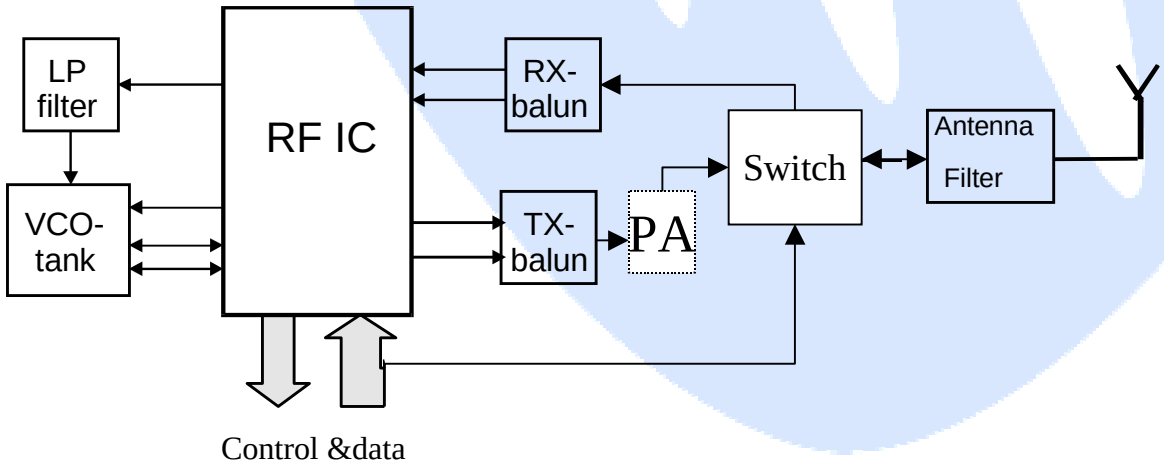
LOW-COST RADIO TECHNOLOGY

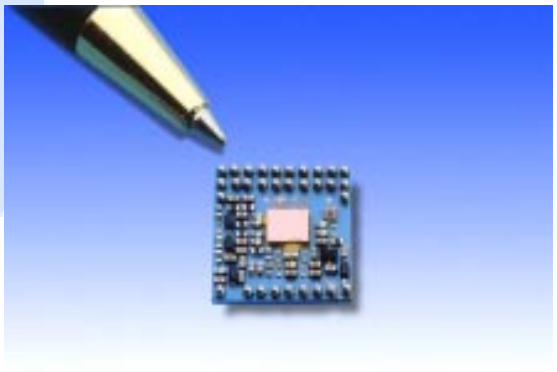
- single chip
- few off-chip components
- main-stream technology
- time-division duplex



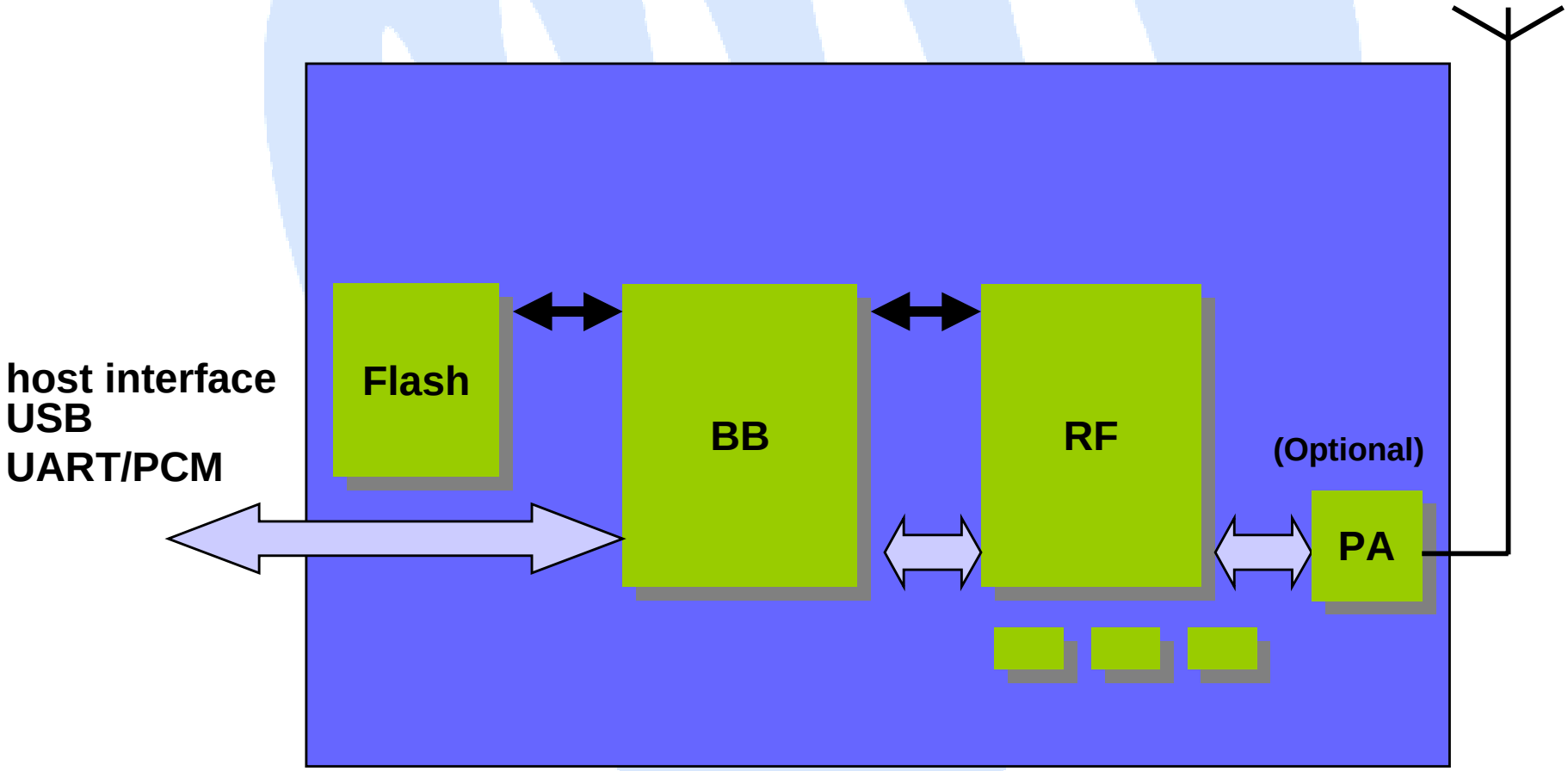
RADIO MODULE EXAMPLE

- filters and baluns integrated into LTCC substrate
- RF IC flip chip mounted
- laser trimming used to optimize performance
- 100mW optional version with PA and optional gain control (- 30 to +20 dBm)
- small outline BGA type package
  - 1mW: 10.2 x 14 x 1.6 mm
  - 100mW: 10.2 x 16 x 1.6 mm

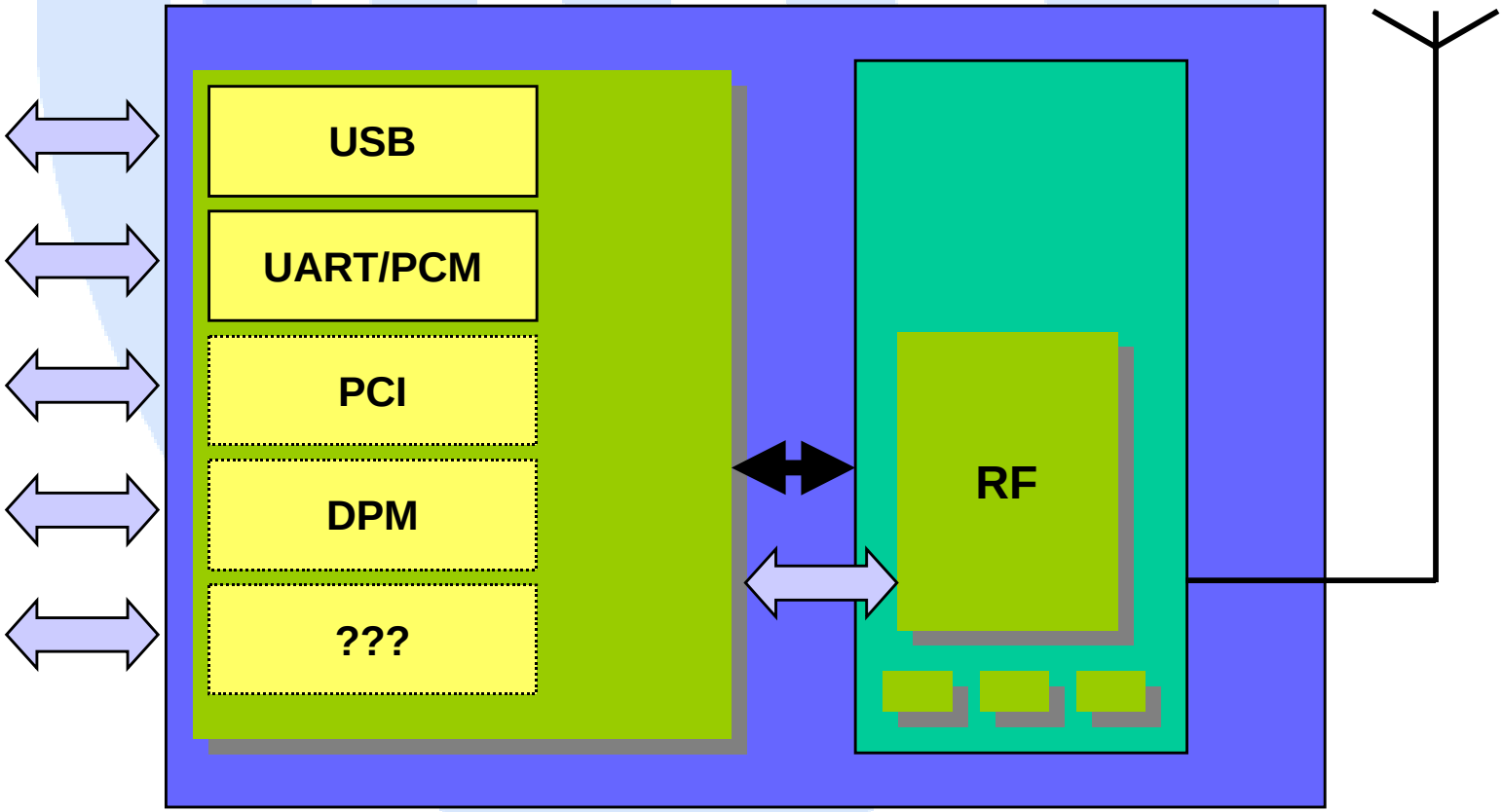




FIRST COMPLETE MODULE



OTHER HOST INTERFACES



BATTERY LIFE TIME

- **Low-power consumption**
  - standby current 0.3 mA
    > 3 months with 600mAh battery
  - voice mode 10 mA (one voice channel)
    > 60 hours
  - data mode average 6 mA (20% utilization)
    > 100 hours
- **Low-power architecture**
  - programmable packet length (else radio sleeps)
  - hold and park modes 60 µA
    - devices connected but not participating
    - device can participate within 2 ms