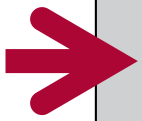
UNIVERSITÄT OSNABRÜCK

Wireless Medium Access Technologies

Bluetooth

Mobile Communication, WS 2014/2015, Kap.3.2

Prof. Dr. Nils Aschenbruck



3.2. Bluetooth

Bluetooth is a **Wireless Personal Area Network** which defines a class of wireless networks providing connectivity between **mobile** or **immobile devices** in the operating space of a person (with a radius of approx. 10 m around the person).

Further Information / Links

Online sources:

- Bluetooth Specifications, **http://www.bluetooth.com/** - **http://www.bluetooth.org/**
- Wireless Resource Center **http://www.palowireless.com/**
  Bluetooth Resource Center **http://www.palowireless.com/bluetooth/**

- many “white papers” about Bluetooth available

Books:

- **Jochen Schiller, Mobile Communications** (2nd edition, Addison-Wesley, 2003)
  (updated online resources available at **http://www.jochenschiller.de/**)

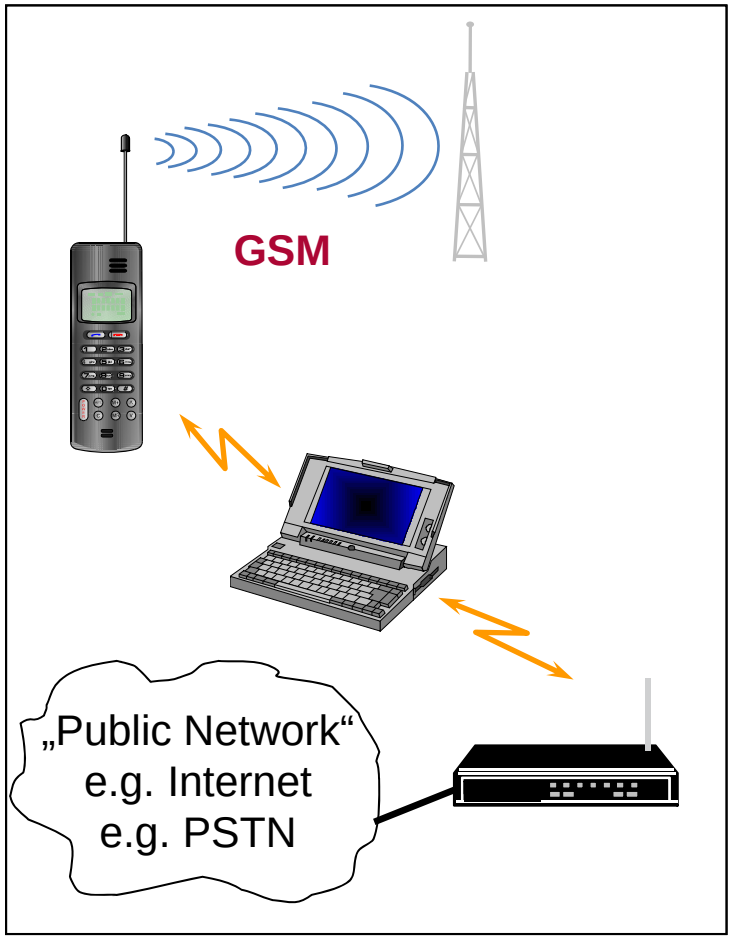
- there are many other books, also dealing with the Bluetooth technology

3.2.1. Wireless Personal Area Networks (WPANs)

With the advent of small electronic devices, the need for communication in the vicinity of a person arises.

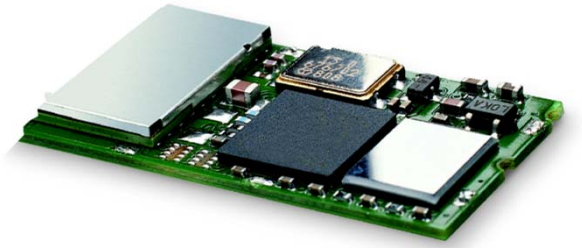
„Wireless Personal Area Networks“ (WPANs) were (and are) developed to fulfill these communication needs. These networks should:

- **Replace cables**
  (cables are clumsy to handle, have various incompatible connectors),
- **Replace infrared communication (IrDA)**
  (WPANs have a higher data rate and require no direct line of sight),
- Enable **seamless communication** of computers, peripherals, handhelds, PDAs, cell phones, ...
  (includes the integration of voice and data),
- Communicate with devices within the **personal operating space** (POS, radius approx **10 m**)
  (for some applications: up to 100 m),
- Have **low power** requirements
  (to be powered with batteries),
- Have functionality similar to a **LAN**
- Support various types of **access points**

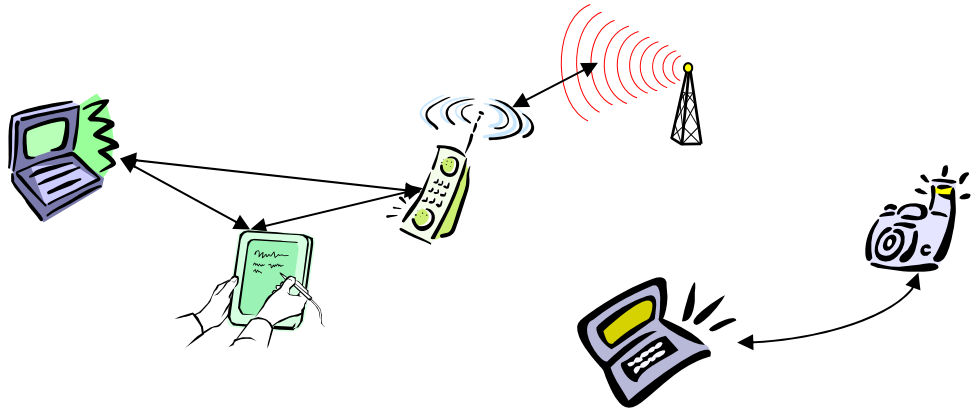


Bluetooth – Basic Idea

- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals,
  - handheld devices,
  - PDAs,
  - cell phones
- replacement of IrDA
- Embedded in other devices, goal: 5€/device (already < 1€)
- Short range (10 m), low power consumption, license-free 2.45 GHz ISM
- Voice and data transmission, approx. 1 Mbit/s gross data rate



One of the first modules (Ericsson).



Bluetooth

The **Bluetooth* SIG** (**Special Interest Group**) is an association of industry leaders in telecommunication driving the development of the Bluetooth WPAN technology.

Bluetooth SPECIAL INTEREST GROUP

http://www.bluetooth.org/

- Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
- Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
- > 10000 members
- Common specification and certification of products

*The Bluetooth technology was code-named after the 10th century Danish king Harald Blaatand (Bluetooth), approx. 950-986, son of the first Danish king Gorm the Old. Harald Blaatand erected a rune stone in Jelling. The stone's inscription says that Harald christianized the Danes and controlled Denmark and Norway. Although originally intended as a code name for the technology, the name stuck.
More info e.g. at http://www.answers.com/topic/bluetooth

3.2.2. The Bluetooth Specification

Overview

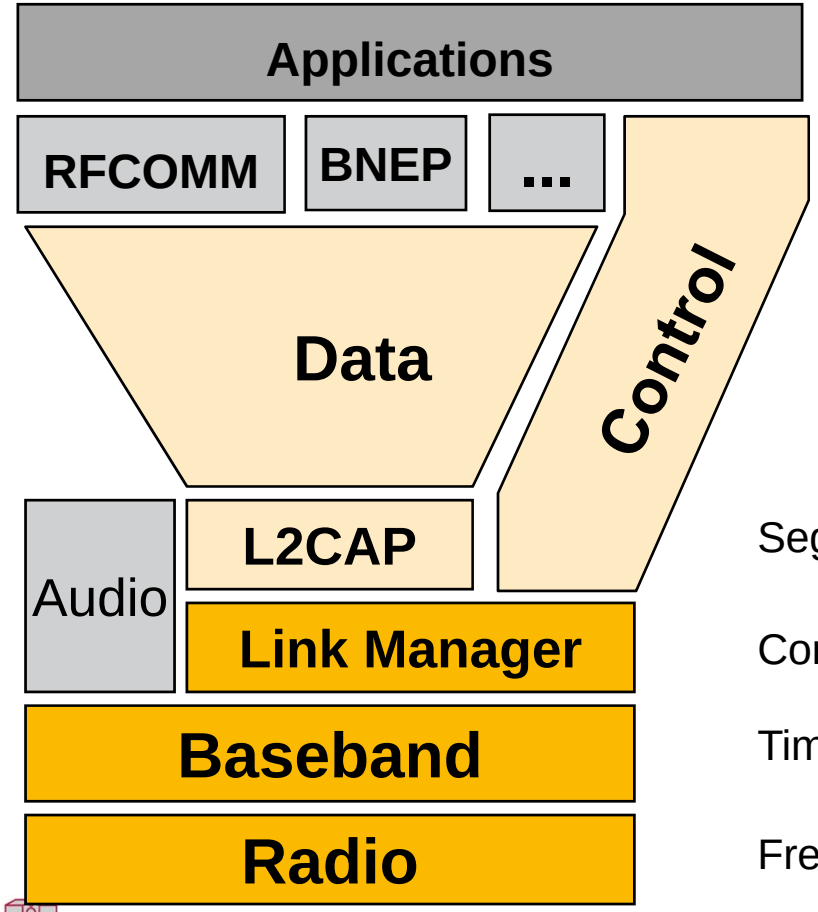
Bluetooth Radio

Baseband

Logical Link Control & Adaptation Protocol – L2CAP

Bluetooth Core Specification:

- Defines the **protocol stack**
- **Physical** definitions (radio) as well as **definition of protocols**
- Specifies **test interfaces** and „**compliance requirements**“



- **RFCOMM:** Emulation of a serial cable
- **BNEP:** Bluetooth Network Encapsulation Protocol (transport of Ethernet frames)
- **SDP:** Service Discovery Protocol
- **...**

Segmentation/reassembly, multiplexing, ...

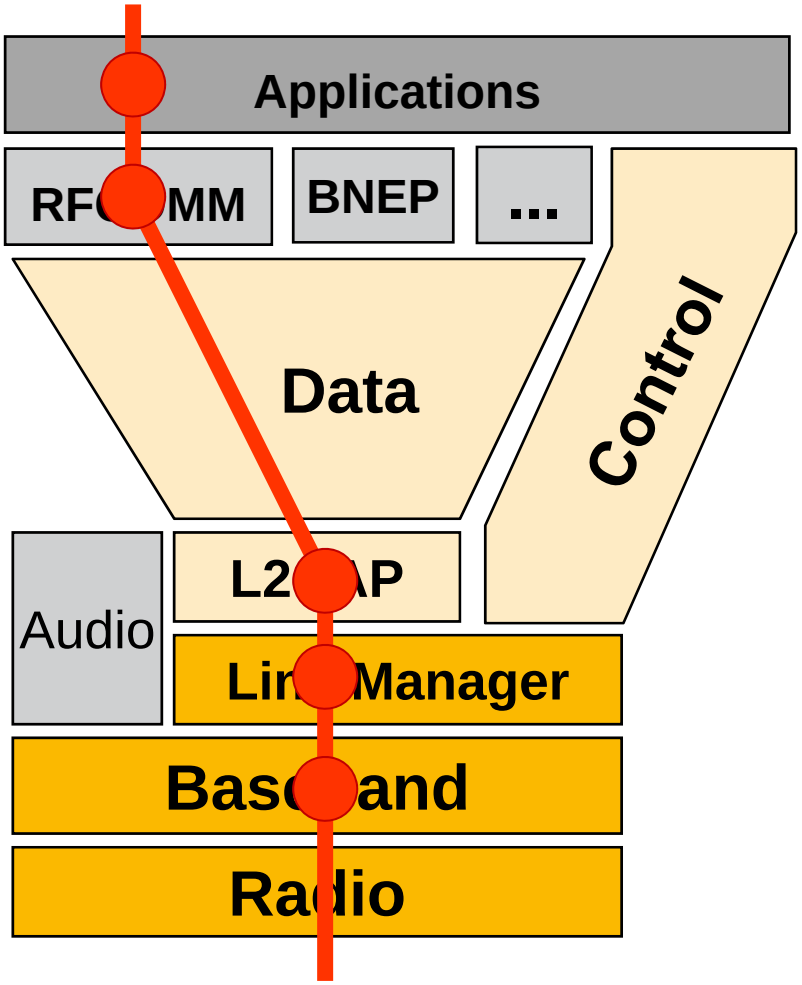
Connection and link management, encryption, ...

Timing, Framing, Medium Access, ARQ, Flow Control

Frequencies, modulation, transmit power, ...

Bluetooth Profiles:

- Standardized solutions for specific **use cases**, e.g.
  - Personal Area Networking Profile
  - File Transfer Profile
  - Serial Port Profile (different from the RFCOMM protocol!)
- Each device supports one or more profiles
- Profiles define vertical cuts through the protocol stack:
  - Which **protocols** are used?
  - What are the **requirements** to be fulfilled?
  - How can devices tell whether another device supports a profile and which features of the profile it implements?
- Profiles are the basis for **interoperability** of Bluetooth applications and for the **certification** of Bluetooth solutions



Bluetooth Radio

Properties of Bluetooth Radio:

- Bluetooth uses the **2.4 GHz ISM band** (ISM = Industrial, Scientific, Medical)

- Three output power classes are defined:
  - Class 3: max. 1 mW
  - Class 2: max. 2,5 mW
  - Class 1: max. 100 mW, power control required

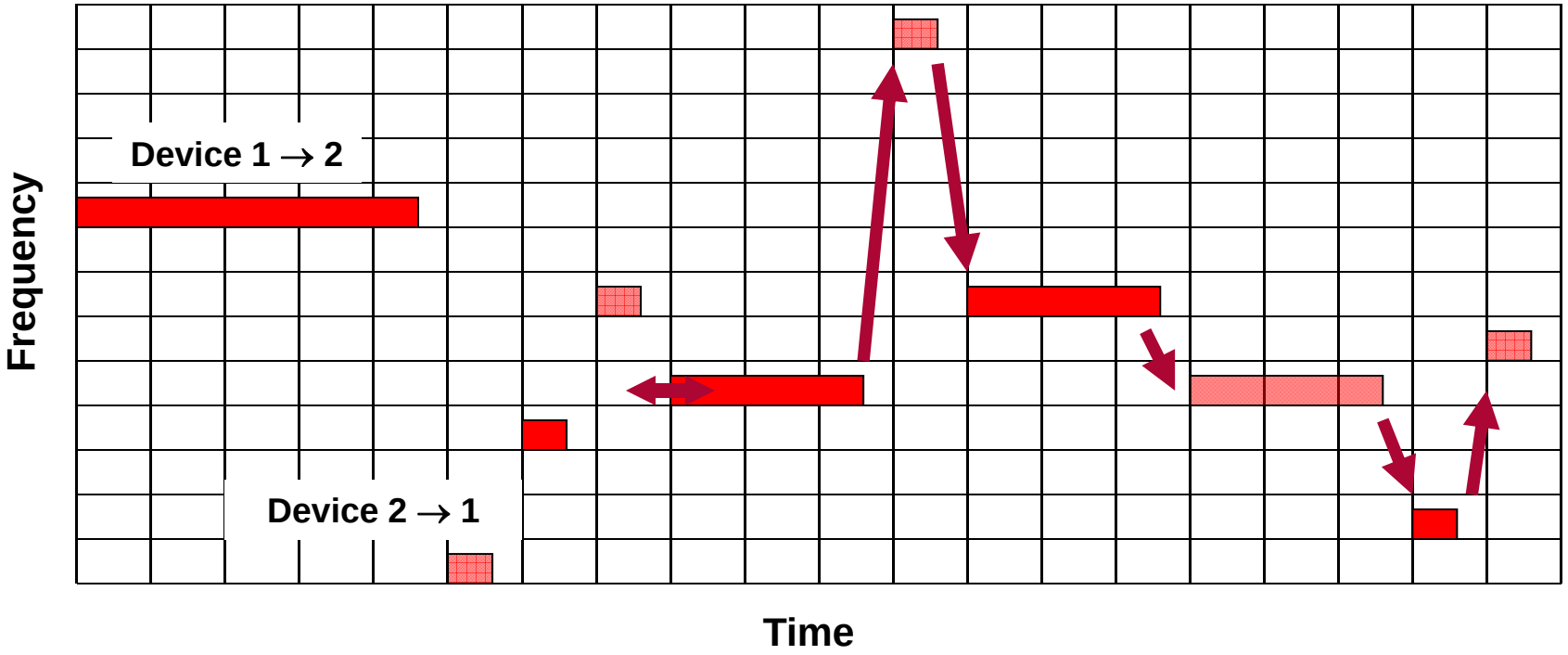
  Range approx. 10 m to 100 m

- Within the frequency band, **79 channels of 1 MHz width are defined**
  - **Frequency Hopping** Spread Spectrum System (up to 1600 hops/s):
    - Sequence of channel changes realizes one virtual channel per piconet
    - Provides resilience against interference und frequency selective fading
  - Raw data rate 1 Mbit/s (Modulation: Gaussian Frequency Shift Keying)
  - Max. **net data rate** 723 kbit/s for data
  - Max. 3 simultaneous full-duplex 64 kbit/s **voice channels**

- **Simple design** to reduce costs: frequency hopping, modulation, receiver characteristics, ...

Frequency Hopping

Communicating devices „hop“ through the frequency space in a coordinated fashion:



Communicating devices must agree in:

- **Hopping Sequence**
- **Timing**

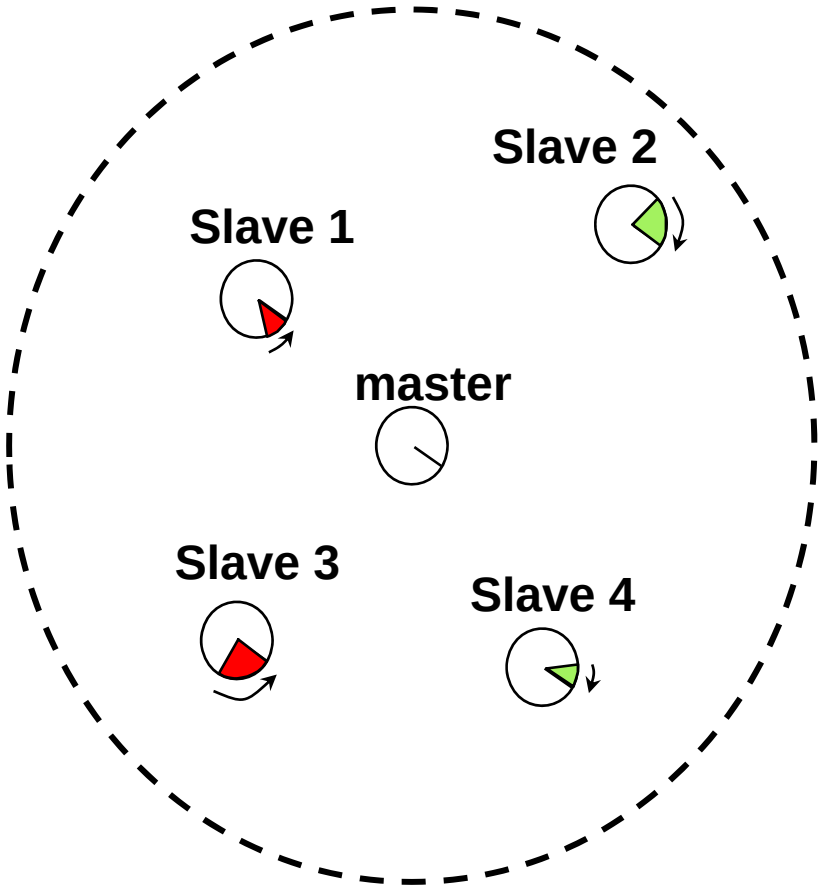
Devices must be in **interference range** and use the **same frequency** at the **same time** in order to provoke a **collision**!
⇒ A few devices using **different hop sequences** do not cause much harm to each other

BD_ADDR = Bluetooth Device ADDRess

Each device in a Bluetooth network has a (globally unique) IEEE 802 **48 bit address (BD_ADDR)** and a **clock (CLK)** running at 3200 Hz.

A Bluetooth network (a Piconet) consists of:
- a **Master** and
- at least one **Slave**

synchronized to each other



The master determines the frequency hopping sequence from:
- its BD_ADDR
- its clock

→ **Pseudo random** hop sequence

Slaves calculate the same sequence using:
- BD_ADDR of the master
- Difference of own and master‘s clock: **clock offset**

Properties of a Piconet:
- **Master/Slave communication** only (no direct communication between slaves)
- Up to 7 active slaves (identified by their AM_ADDR = active member address)
- Additional inactive “parked” slaves (up to 255, using PM_ADDR = park mode address))

Bluetooth Medium Access Control (MAC)

In a piconet:

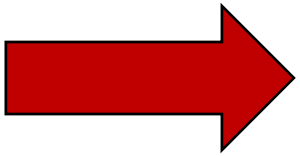
- All devices are **synchronized** to the master
- At each **point in time** the hop sequence determines a **frequency** to send or receive on

Only **one device** of a piconet may send at a time, otherwise the devices interfere with each other!
A **medium access method** is needed in order to use the medium efficiently!

Local Area Networks often use random access methods (e.g. CSMA/CA, CSMA/CD) that may cause **collisions** on the medium.

Due to collisions, random access methods cannot guarantee packet delivery within a given time bound.

But: Bluetooth was designed to transport **voice calls**. Given the restricted overall bandwidth of Bluetooth, it is hard to fulfill the hard requirements on **delay** and **jitter** using random access methods.



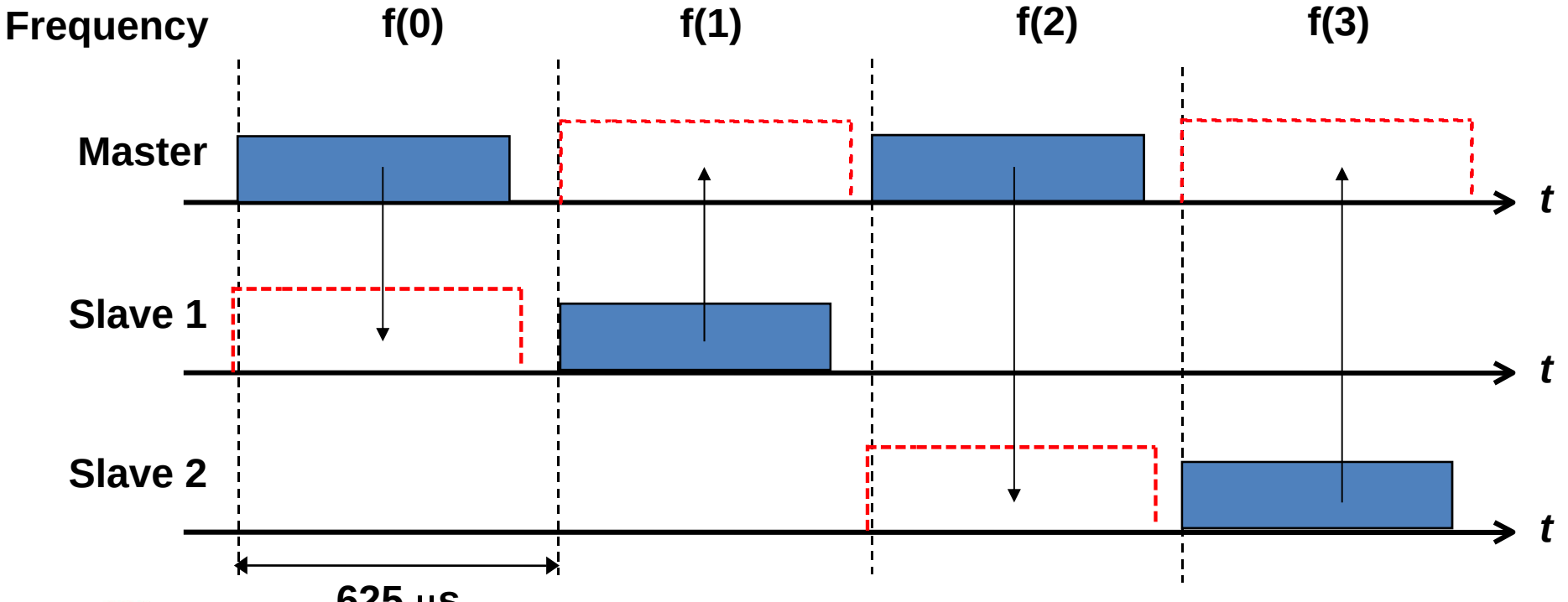
Bluetooth uses a simple, contention-free „Polling“-MAC:

Time-Division-Duplex (TDD)

Time-Division-Duplex (1)

- The master determines **slots with fixed length** (625μs). Additionally, each slot is assigned a frequency using the hop sequence
- The **master** may send a unicast packet to a specific slave or a broadcast packet to all slaves in the **even slots only**
- In the **odd slot** subsequent to a master transmission, the **slave addressed by the master** may respond

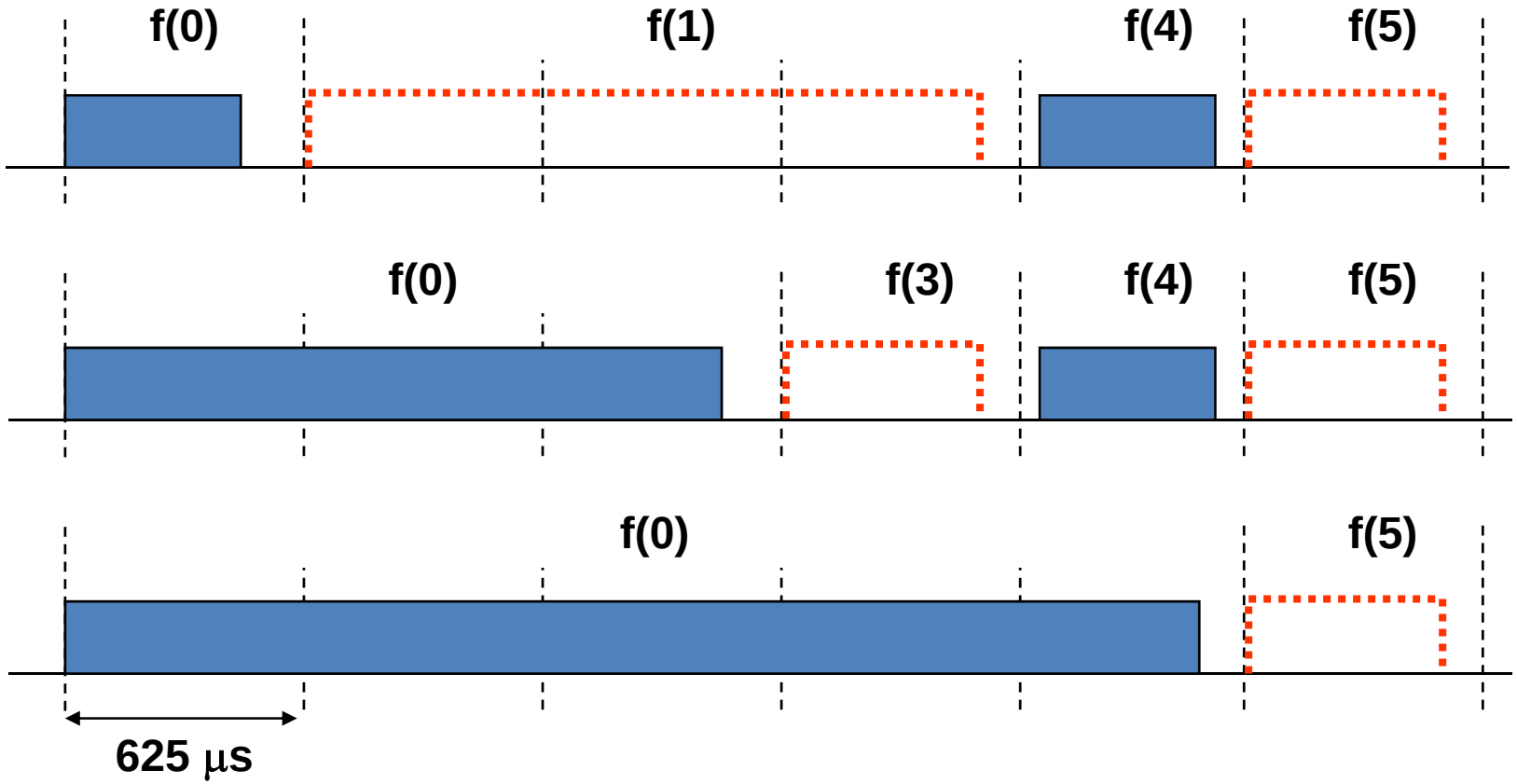
A slave may **never** send on its own, it always has to be **polled** (using some packet) by the master!
It is the duty of the master to ensure that slaves are polled at times.



Time-Division-Duplex (2)

In order to increase efficiency, packets longer than a single slot were introduced:

- The odd/even slot rule only allows packets spanning an odd number of slots
- Bluetooth uses **1, 3 and 5 slot packets**



Frequencies cannot be switched instantly. In order to avoid performance losses due to frequency switching, packets are always sent on a **single frequency**.

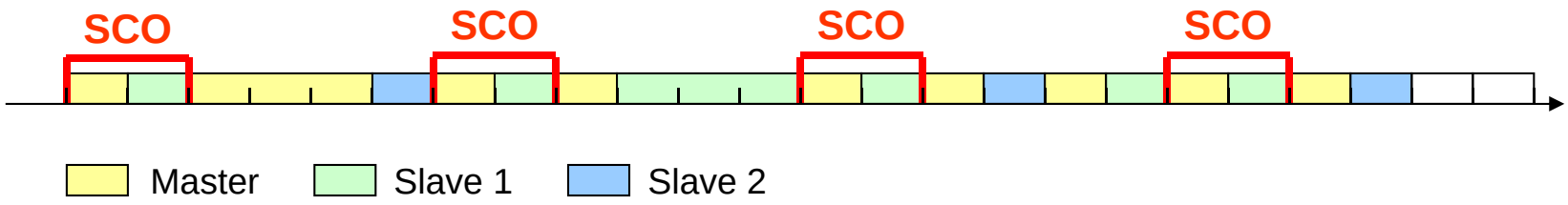
Types of Links

Bluetooth supports two types of links:

- **Synchronous Connection Oriented (SCO) link** (typically used for voice)
  - **Point-to-point full duplex connection** between master and slave
  - Master **allocates** slot pairs using a fixed period
  - May use a code insensitive to random bit errors (CVSD, Continuous Variable Slope Delta Modulation)

- **Asynchronous Connectionless (ACL) link** (typically used for data)
  - **No reservation of slots** (master decides which slave to address)
    - Slots reserved for SCO have priority
  - **TDD scheme**: A slave may only send when polled by the master
  - **Packet header** indicates which slave is addressed

In case of bad link conditions, it may be beneficial to secure packets against transmission errors by applying **Forward Error Correction** (**FEC**).



Packet Types

Depending on the link type, the following packet types are defined:

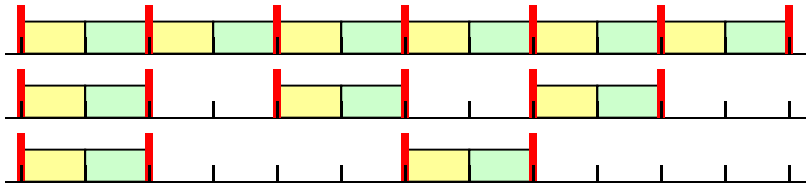
- **Asynchronous Connectionless (ACL) link**
  - **DM1, DM3, DM5**, 2/3 Rate FEC, CRC, 1, 3 and 5 slot packets
  - **DH1, DH3, DH5**, no FEC, CRC, 1, 3, and 5 slot packets
  - **AUX1**, no FEC, no CRC, 1 slot packet
  - Max. data rates in kbit/s:

	Symm.	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

Symmetric: DM3/DM3

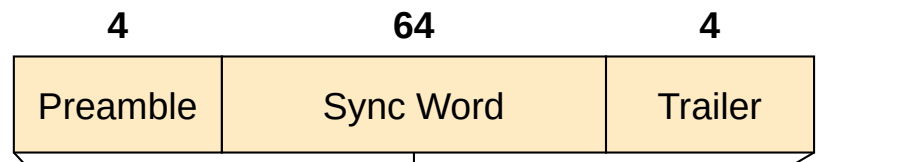
Asymmetric: DM3/DM1

- **Synchronous Connection Oriented (SCO) link**
  - **HV1**, 1/3 Rate FEC, 64 kbit/s full duplex
  - **HV2**, 2/3 Rate FEC, 64 kbit/s full duplex
  - **HV3**, no FEC, 64 kbit/s full duplex



  - **DV**, 64 kbit/s audio (SCO) full duplex + 57,6 kbit/s data (ACL) symmetric
  - **DM1**, used for link management

Packet Format

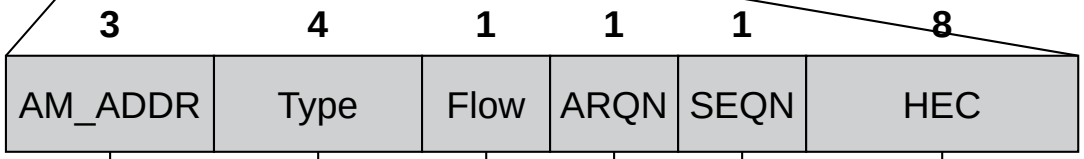


Sync Word

- Identifies the piconet (based on master's BD_ADDR)
- Construction improves correlation properties

CRC – Error Check for Payload

1/3 rate FEC



Active Member Address
0: Piconet Broadcast
1-7: Slave Address

Header Error Check

Sequence Number

Automatic Repeat Request
0: NAK
1: ACK

Packet Type

Flow Control
0: STOP
1: GO

Automatic Repeat Request (ARQ)

What happens if a packet is not received at all or is not received correctly?

Common practice for low error rates experienced in wired networks (e.g. Ethernet):

- Discard packets with bad CRC
- Higher layers are required to correct the error (e.g. link layer or transport layer)

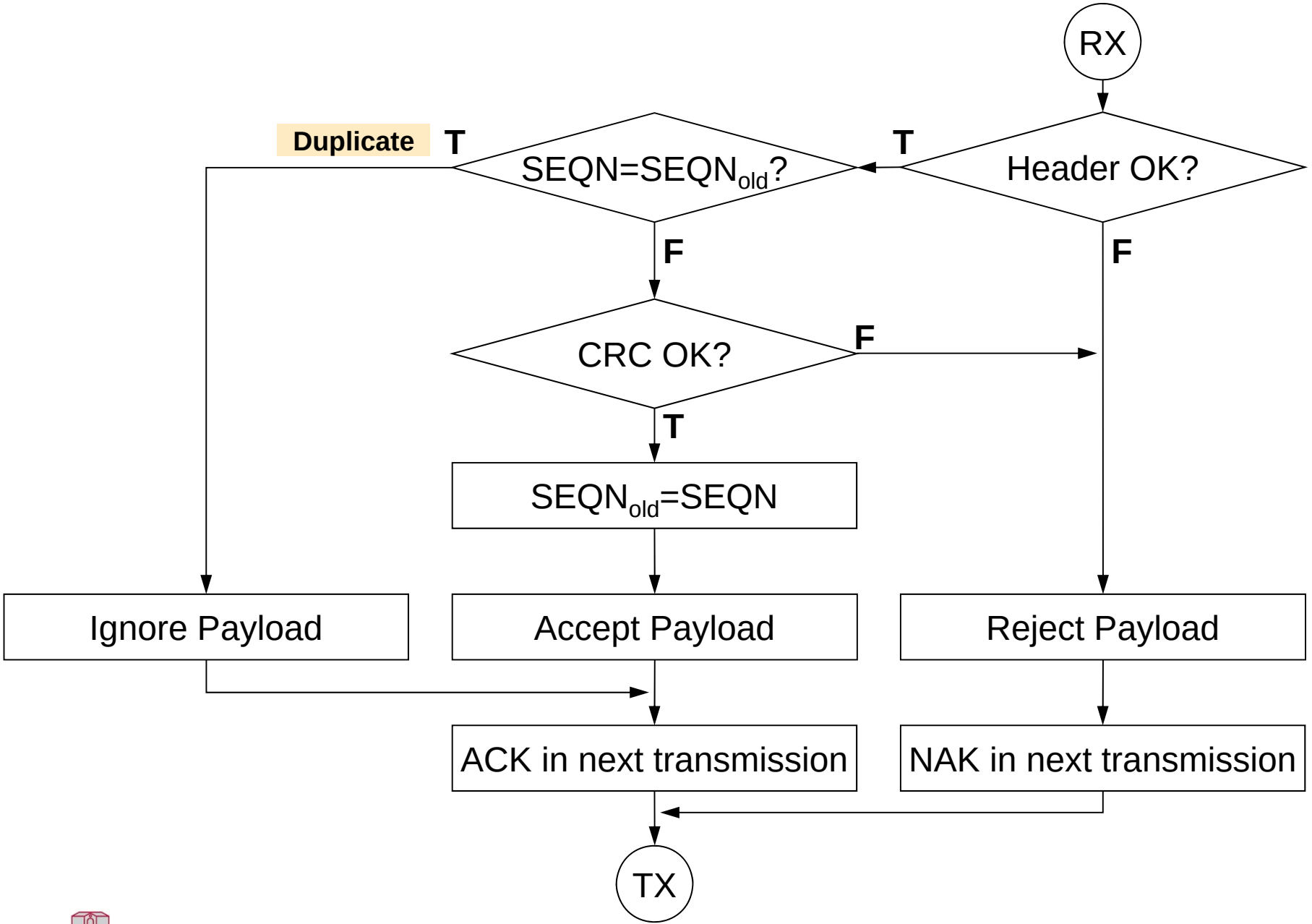
Error rates in wireless communication system are much higher:

- Higher layer correction is too slow in many cases
- Higher layers (TCP in particular) may assume that packet losses are caused by congestion instead of packet errors
  → Congestion avoidance reduces data flow erroneously

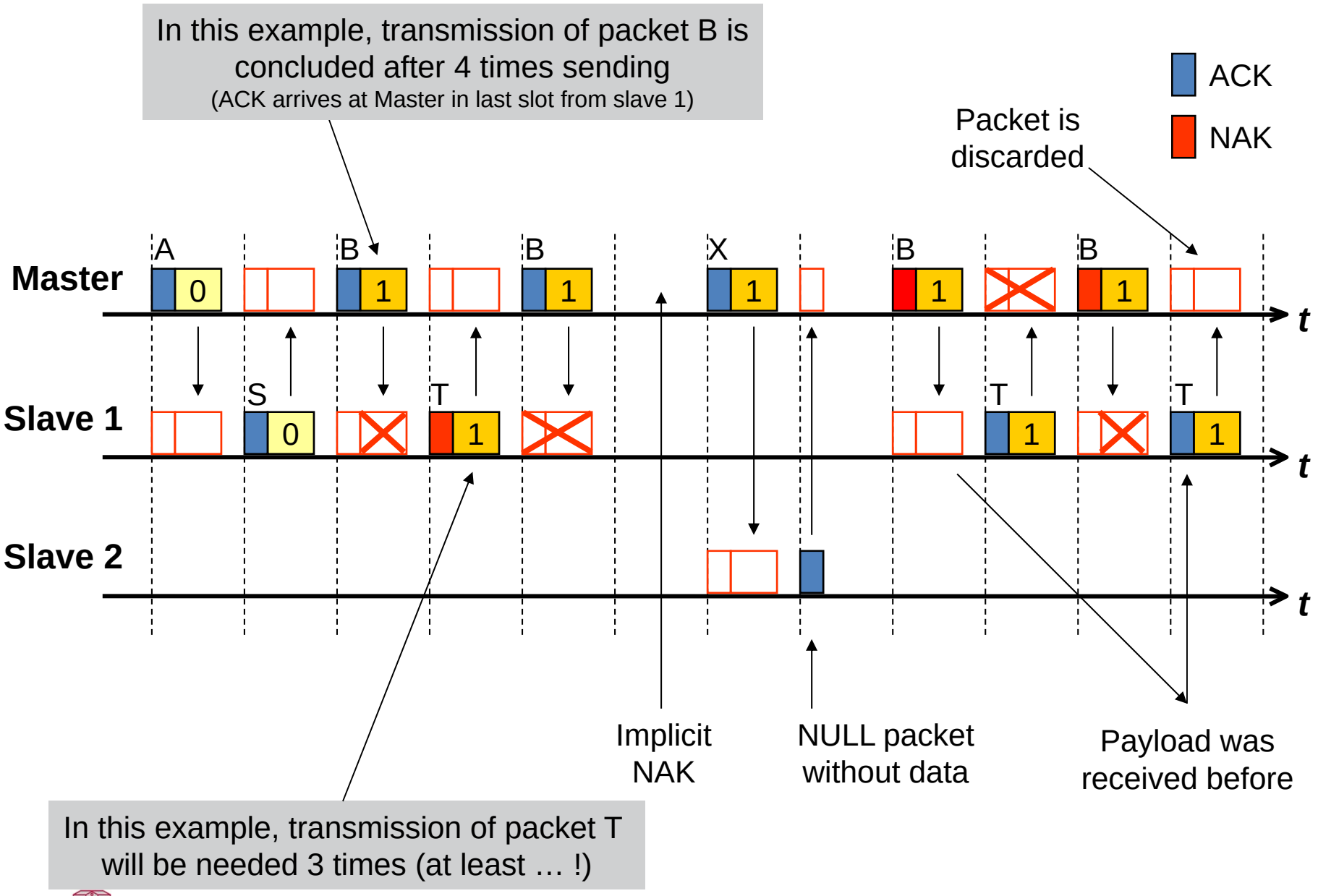
Bluetooth baseband uses a **fast automatic repeat request** (**Fast ARQ**) for ACL data packets:

- **Piggy-backed** ARQN-Bit in the header of the return packet
  - If there is no data to send, a short packet without data (NULL or POLL) is used
  - If the slave sends no return packet, **NAK is implicit**
- Acknowledgement occurs as **fast** as possible
  - Master-to-slave: ACK in the next odd slot following the current transmission
  - Slave-to-master: ACK at next poll of the slave
- Duplicate packets filtered by **alternating sequence numbers**
  - Sequence number switches (0 → 1, 1 → 0) for each new packet

The Bluetooth Receive Protocol for Data Packets



ARQ: Example

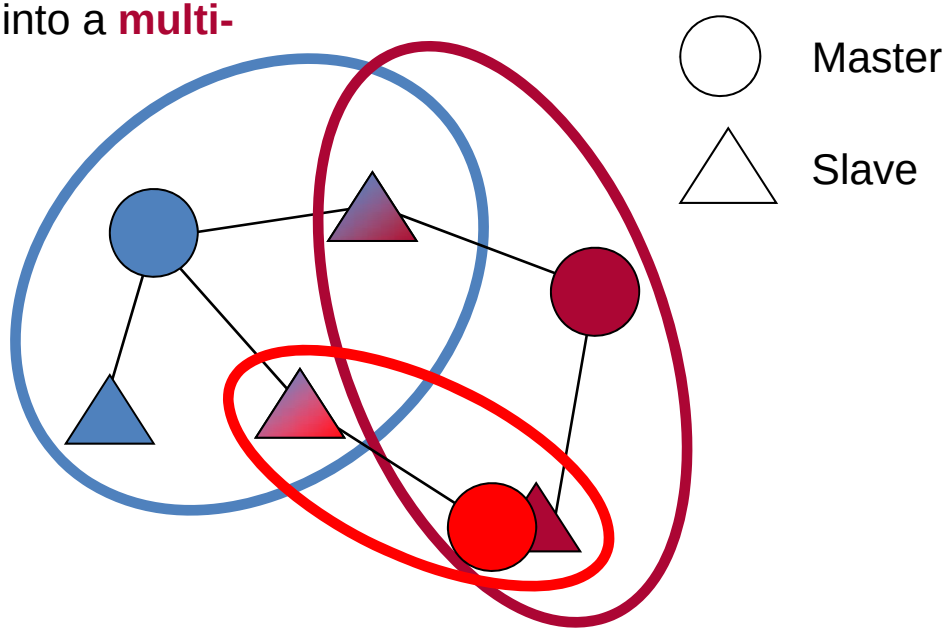


Multi-Hop Bluetooth Networks: Scatternets

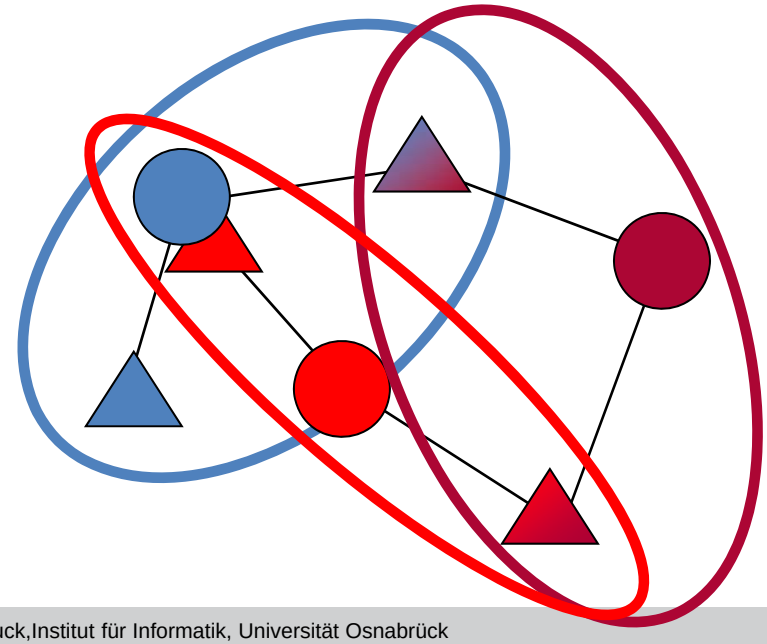
Multiple Bluetooth piconets may be combined into a **multi-hop Bluetooth network**, a „**scatternet**“.

A Bluetooth device connected with several other devices may be:

- A master to all connected devices (slaves)
- A slave to all connected devices (masters)
- A combination thereof: master to connected slaves and slave to different masters



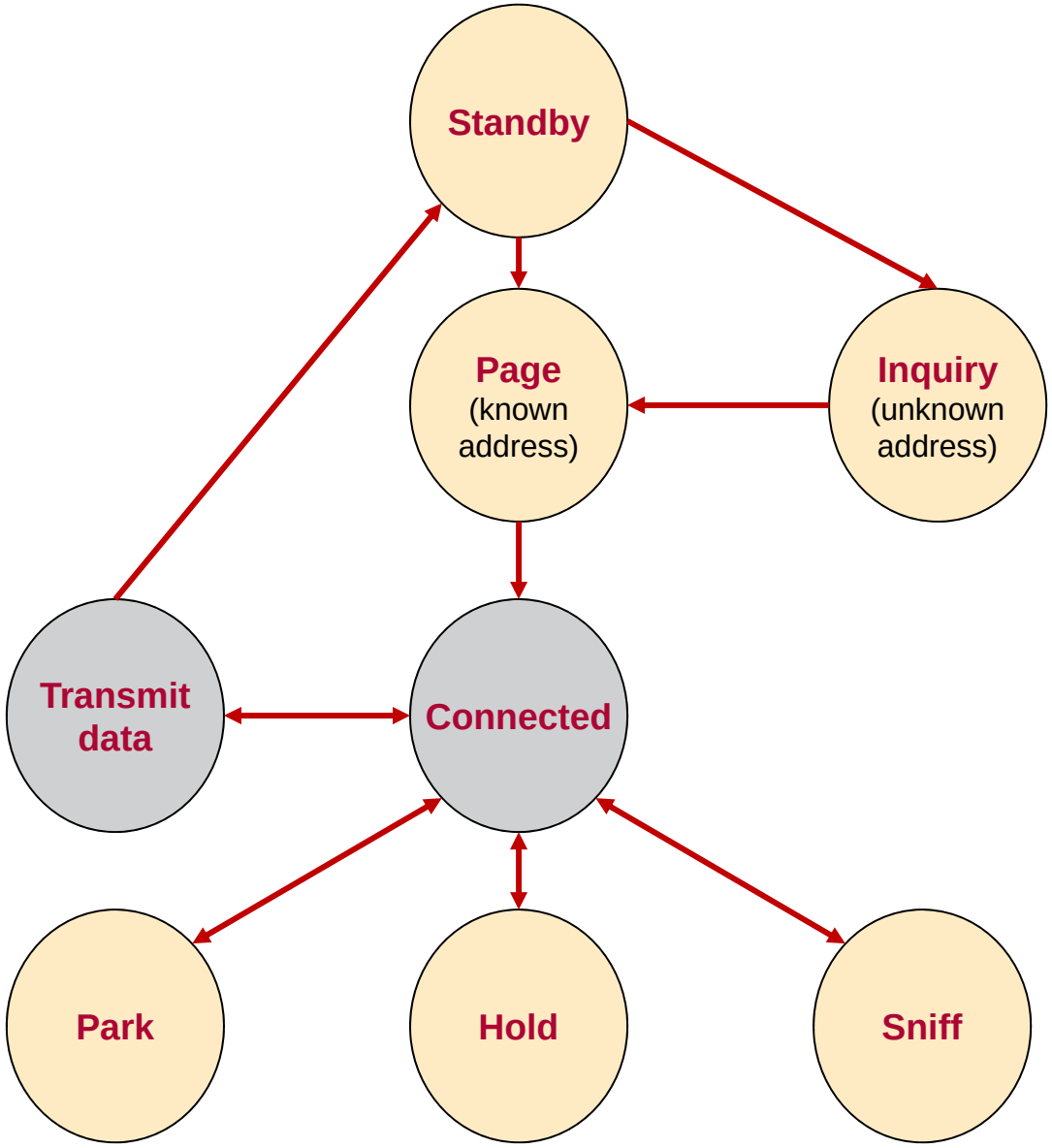
- The same physical topology can be achieved using different master/slave assignments.



Each device can only participate in one piconet at each point in time

Devices switch between piconets using a coordinated time division multiplex scheme

Connection Management in the Piconet



Not connected

Connection establishment

Active

Power saving

Releases Active Member Address

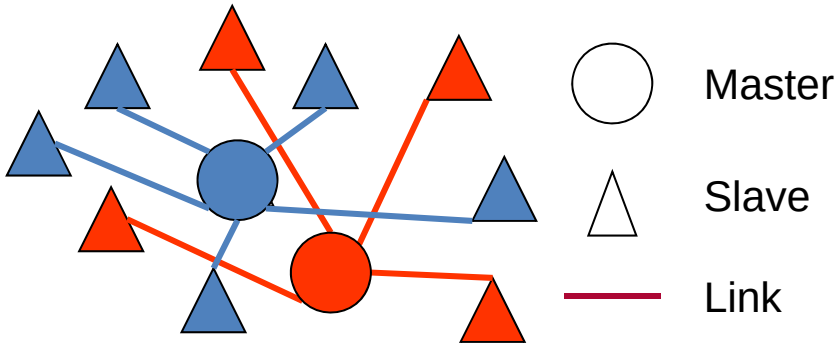
Keeps Active Member Address

Connection Establishment (1): Page

Being in communication range is not sufficient to establish a link!

Master and slaves of a piconet must agree in:

- **Hop Sequence**
- **Timing**



New slaves must get to know these parameters from the piconet's master!

Page Scan (passive role, future slave):

- Each **1.28 s** (or 2.56 s), a device scans **one** of its 32 **page frequencies** for approx. 11 ms.
- The slave responds if it is hit by a paging device during the scan: initial synchronization
- The **32** page frequencies are based on the device's **BD_ADDR.**

Paging (active role, future master):

- The master sends **page trains** using **16** of the 32 page frequencies of the slave.
- The page train is **repeated 128** (or 256) **times**, this corresponds to the **1.28 s** (or 2.56 s) needed to **hit** the slave's **scan window**.
- If no answer is received, the **remaining 16** frequencies are tried.
- The **master/slave roles** may be **switched** after a successful connection establishment.

Connection Establishment (2): Inquiry

Paging only connects to devices that are already known:

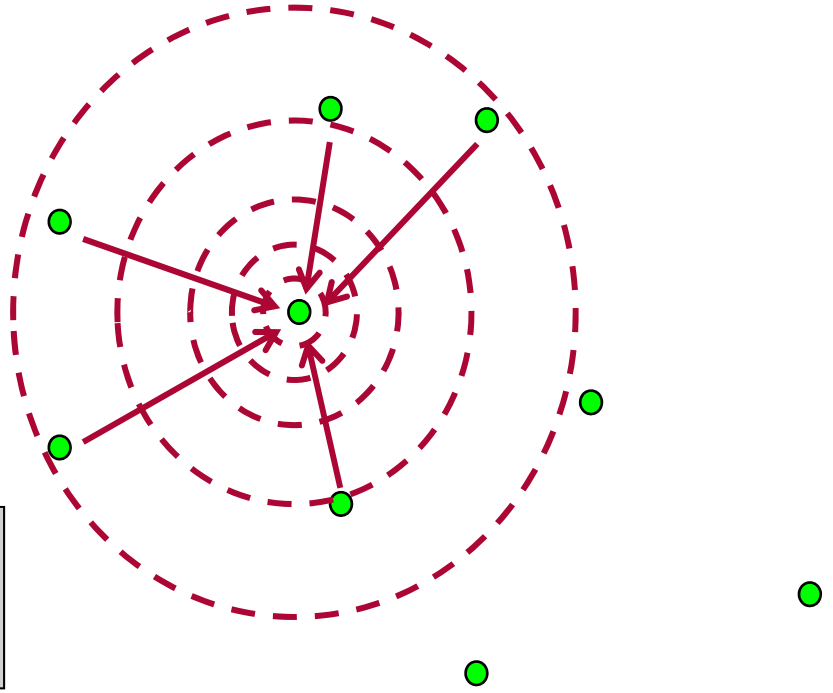
Paging needs the BD_ADDR of the slave

Using **inquiry**, a device may search for other Bluetooth devices in range:

- Similar to page procedure
- Detectable devices periodically enable **inquiry scan**
- Devices searching other devices switch between two **inquiry train repetitions**

An inquiry response contains:

- **BD_ADDR** (used for paging)
- Device **clock** (speeds up paging)
- **Class of device** (e.g. Access Point, Audio, Telephony, ...)



Inquiry does not establish a connection!
Devices must page the BD_ADDR obtained from the inquiry response if a connection is desired.

Power Saving Modes

In order to save power, an **active slave** always minimizes its listen time:

- It listens for a **valid access code** only at the beginning of each **even slot**.
- If an access code is received, it has to listen to the **packet header** in order to figure out the intended recipient. Otherwise, disable the receiver till the next even slot.
- If the **packet** is for the slave, receive the packet. Otherwise, disable the receiver for the duration of the packet.

SNIFF mode:

short-term, periodical

- reduces the duty-cycle even further
- Master and slave agree on a periodic subset of even slots in which the slave listens (so called **SNIFF interval**)

HOLD mode:

medium term, once

- a slave may want to cease activity in a piconet **for a specific time** (for inquiry or page, for activity in another piconet, to save power)
- slave and the master agree on a **HOLD interval**. After the interval has passed, the slave **resynchronizes** to the master

PARK mode:

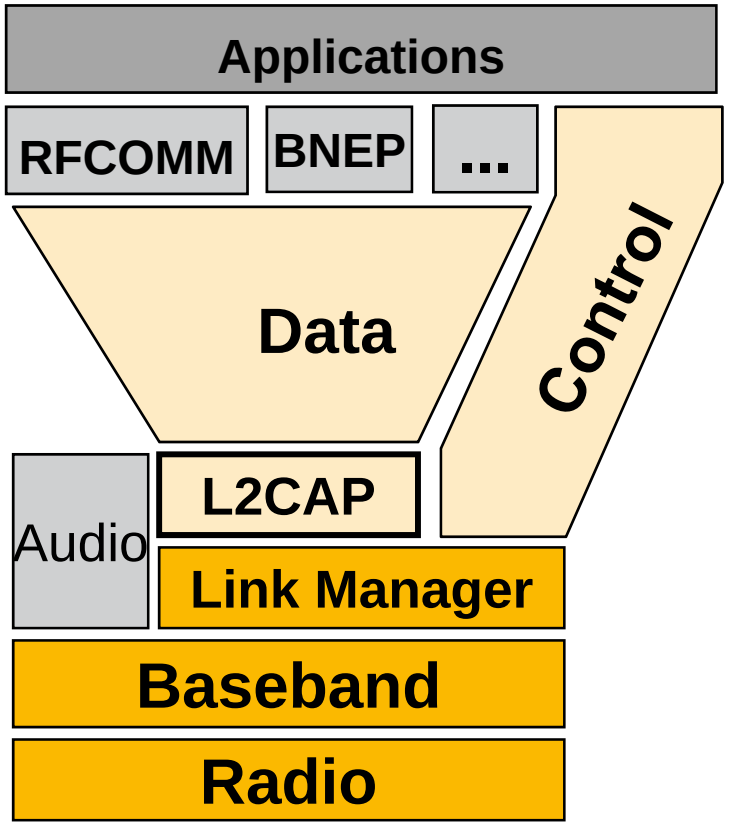
long term, once

- a slave wants to cease activity in a piconet **for a longer time**
- release AM_ADDR, receive PM_ADDR (park mode address)
- activity only for beacons of master (broadcast traffic, timing to be negotiated)

L2CAP – Logical Link Control & Adaptation Protocol

Common network protocols (e.g. IP) are not optimized for directly interfacing baseband:

- **Small packets**
  - Largest baseband packet (DH5): **341 data bytes**
  - Largest Ethernet packet: **1500 data bytes**
  - Use of packet types may depend on link quality:
    - **Good link**: 1500 bytes in 4 x DH5 + 1 x DH3
    - **Average link**: 1500 bytes in 7 x DM5
- No provisions to use more than one user protocol on top of baseband
- Protocols know nothing about **master and slave** roles or Bluetooth **connection establishment**



Logical Link Control & Adaptation Protocol (L2CAP) has two main purposes:

- **Logical Link Control** (i.e. link layer protocol)
- **Adaptation**: provide larger packets, abstraction of master/slave principle, …

3.2.3. Bluetooth Profiles

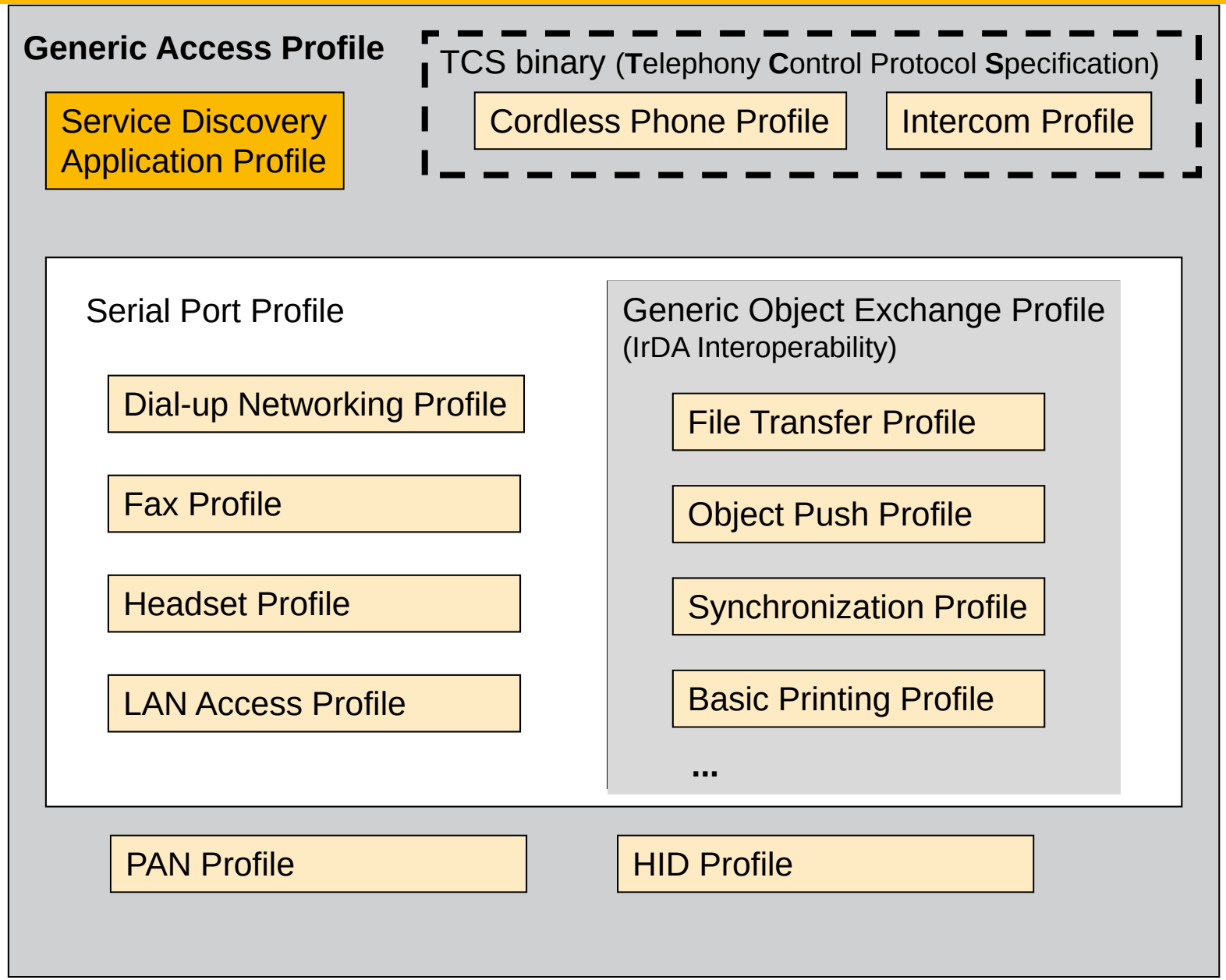
Bluetooth Profiles are standardized **solutions** for specific **use cases**. They are the base for **interoperability** of Bluetooth applications and for the **certification** of Bluetooth solutions.

Overview of the Bluetooth Profiles

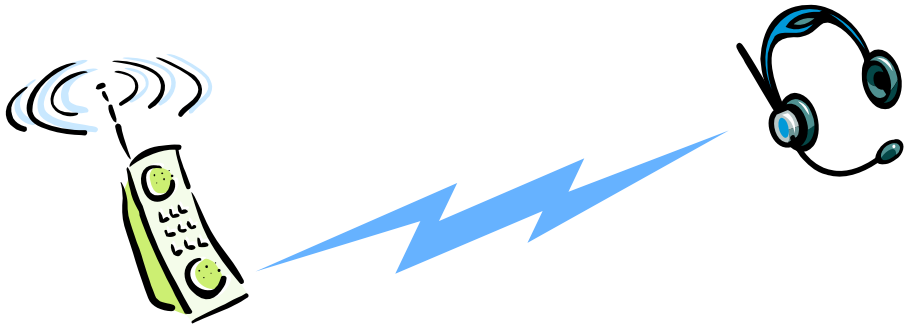
One Example: Headset Profile

(PAN Profile + BNEP see 3.2.5. Further Information)

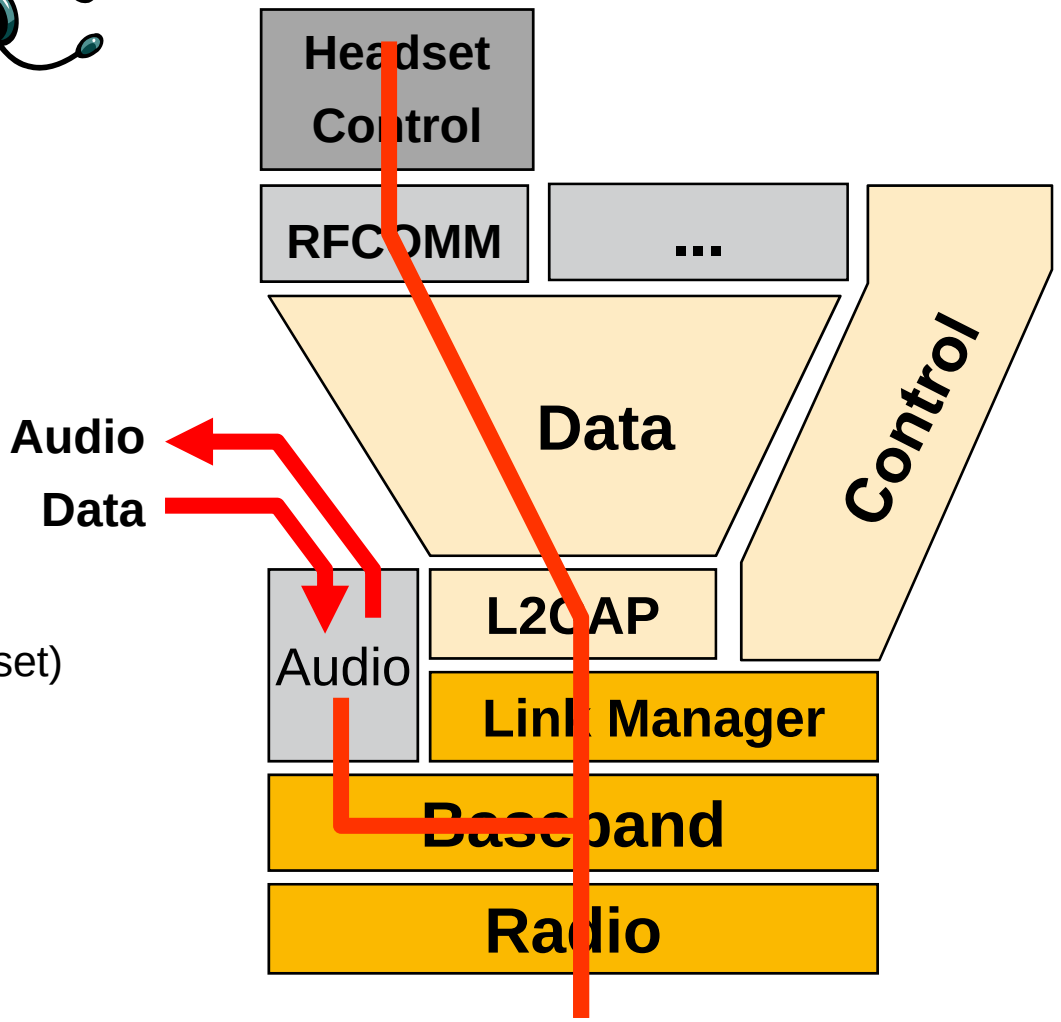
Overview of the Bluetooth Profiles



One Example: Headset Profile



- **Full duplex audio (SCO)**
  - Incoming and outgoing calls
- **Control using RFCOMM**
  - AT commands (modem command set)
  - Call indication
  - Supports keys on headset
  - Volume control by the remote side



3.2.4. Bluetooth Version Overview (1)

Bluetooth 1.0, 1.0B – December 1999

- first version(s) – many interoperability problems

Bluetooth 1.1 – February 2001

- many errors of 1.0/1.0B fixed
- RSSI - Received Signal Strength Indicator

Bluetooth 1.2 – November 2003

- eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
- Adaptive Frequency-hopping spread spectrum (AFH)

IEEE WPAN Group 802.15
IEEE Standard 802.15.1-2002
(based on Bluetooth version 1.1)
IEEE Standard 802.15.1-2005
(based on Bluetooth version 1.2)

Bluetooth 1.0 – 1.1 – 1.2 working with **nominal data rate of 723 kbit/s**

Bluetooth 2.0 – November 2004

- Enhanced Data Rate (EDR) of **up to 3.0 Mbps (nominal)**
- Lower power consumption, improved BER (bit error rate) performance

Bluetooth 2.1 + EDR – August 2007 (aka Lisbon Release)

- new features: secure simple pairing, Quality of Service

Bluetooth Version Overview (2)

Bluetooth 3.0 + HS (High Speed) – April 2009 (aka codename “Seattle”):

- **originally intended:** adopting Ultrawideband UWB radio tech.

- HS achieved by AMP: alternate MAC/PHY
- inclusion of the **802.11** Protocol Adaptation Layer (PAL)

- (finally no inclusion of UWB)

Bluetooth 4.0 + EDR – June 2010:

- provisional names *Wibree* and *Bluetooth ULP* (Ultra Low Power) – meanwhile abandoned

specification includes:

- classic BT
- BT high speed (based on WiFi)
- BT low energy protocols (aims at Bluetooth in gadgets, battery lasting several years)

(first Bluetooth 4.0 products available since mid 2011)

Bluetooth 4.1 – Dec. 2013:

- adding new features and benefits
- Internet of Things

3.2.5. Bluetooth Low Energy, Bluetooth LE, Bluetooth Smart

- originally introduced under the name Wibree by Nokia in 2006
- included as part of Bluetooth 4.0
- **not backward-compatible** with classic Bluetooth
  - dual mode devices possible
  - same 2.4 GHz radio frequencies as Classic Bluetooth
    - **dual-mode devices** can share a single radio antenna
  - LE uses a simpler modulation system.
- first smartphone to implement the BT Smart was the iPhone 4S
  - Label: “Bluetooth Smart Ready“

- **Profiles / Markets**:
  - health care (temperature measurement, blood glucose, blood pressure, …)
  - sports (heart rate, bicycle sensors, running speed, location, …)
  - proximity sensing (e.g., iBeacon)
  - Internet of Things

- **More details**:
  - Bluetooth 4.1 Core Specification, 2013, www.bluetooth.org
  - J. Decuir: „Introducing Bluetooth Smart: Part 1: A look at both classic and new technologies “, IEEE Consumer Electronics Magazine, Vol. 3 (1), Jan. 2014, pp. 12-18, http://dx.doi.org/10.1109/MCE.2013.2284932

Bluetooth Smart – Some Details

Goal: enable a market of "appcessories"

- small and simple devices that can be peripherals for smartphones and other mobile devices

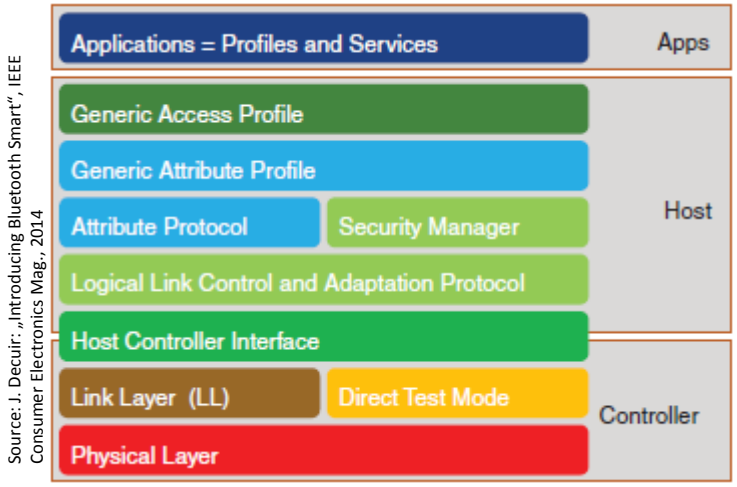
Design Features:

- new (wireless) PHY derived from Bluetooth BR
- recycling some critical components, e.g. multiplexer L2CAP
- new advertising mechanism for efficient device and discovery
- new asynchronous connectionless MAC for low latency and fast transactions
- new generic attribute protocol (ATT), which in turn supports a simple client/server model
- a new generic attribute profile (GATT) provides an efficient way of collecting data from sensors.
- **NOT** data throughput

Range	~150 m open field
Output power	~10 mW (10 dBm)
Max current	~15 mA
Latency	3 ms
Topology	Star
Connections	>2 billion
Modulation	GFSK @ 2.4 GHz
Robustness	Adaptive frequency hopping, 24-b CRC
Security	128-b AES CCM
Sleep current	~1 µA
Modes	Broadcast, connection, event data models reads, and writes

Note: Items marked in blue are defined in the specification; other items are implementation specific.

Source: J. Decuir: „Introducing Bluetooth Smart", IEEE Consumer Electronics Mag., 2014



Source: J. Decuir: „Introducing Bluetooth Smart", IEEE Consumer Electronics Mag., 2014

Bluetooth Smart – Technical Specification

Bluetooth® SMART

Technical Specification	Classic *Bluetooth* technology	*Bluetooth* low energy technology
Radio frequency	2.4 GHz	2.4 GHz
Distance/Range	10 meters	10 meters
Over the air data rate	1-3Mbps	1Mbps
Application throughput	0.7-2.1 Mbps	0.2 Mbps
Nodes/Active slaves	7- 16,777,184	Unlimited
Security	64b/128b and application layer user defined	128b AES and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive fast frequency hopping
Latency (from a non connected state)		
Total time to send data (det.battery life)	100ms	<6ms
Government regulation	Worldwide	Worldwide
Certification body	Bluetooth SIG	Bluetooth SIG
Voice capable	Yes	No
Network topology	Scatternet	Star-bus
Power consumption	1 as the reference	0.01 to 0.5(depending on use case)
Peak current consumption	<30 mA	<15 mA (max 15 mA to run on coin cell battery)
Service discovery	Yes	Yes
Profile concept	Yes	Yes
Primary use cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, etc.	Mobile phones, gaming, PCs, watches, sports & fitness, healthcare, automotive, home electronics, automation, Industrial, etc.

Source: Bluetooth Low Energy-Technical Facts, http://www.bluetooth.com

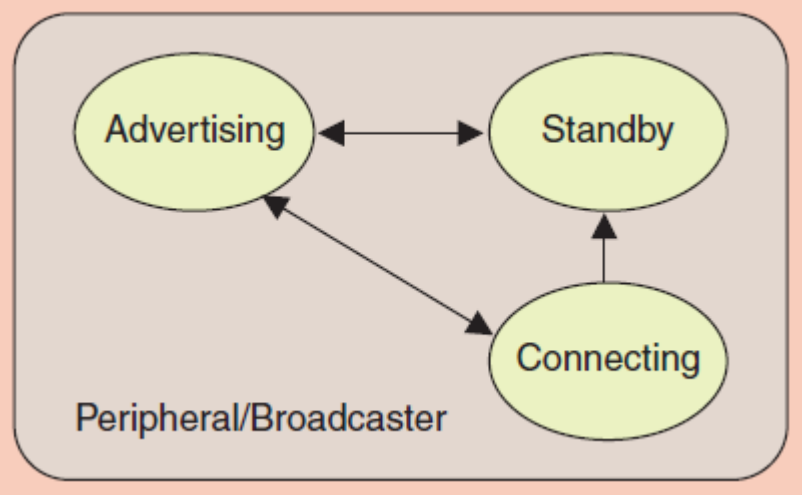
Bluetooth Low Energy (aka Smart)

- Lower power
- Lower latency
- Lower throughput
- Lower range

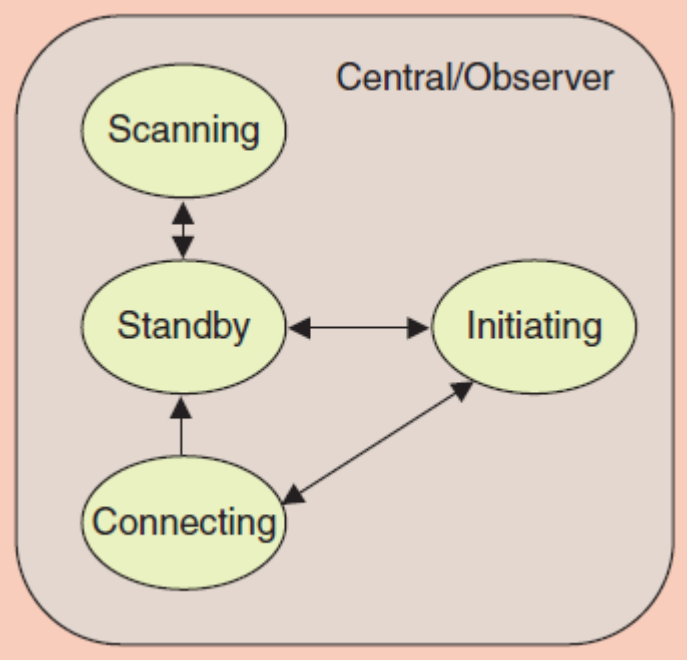
Source: Janc, Rymanowski: „Bluetooth Low Energy on Android“, Androids Builders Summit 2013

Bluetooth Smart – Device States

Sensor Device

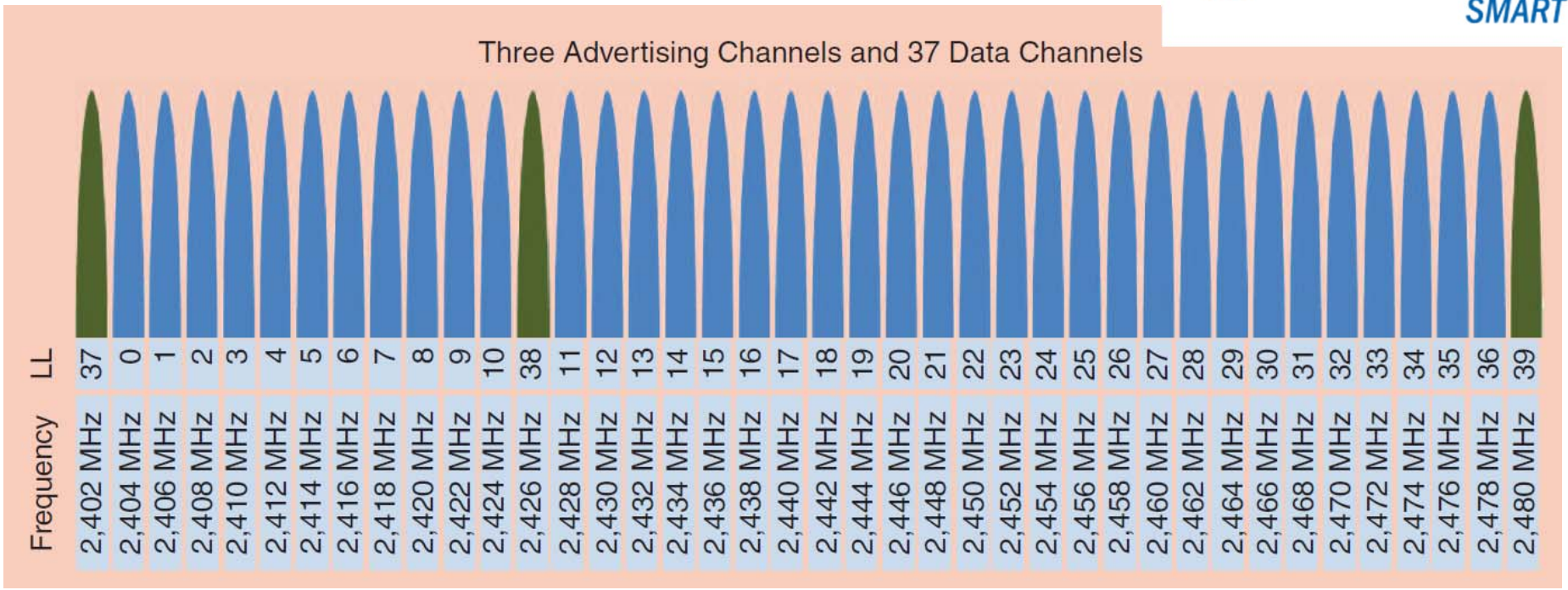


Collector Device



Source: J. Decuir: „Introducing Bluetooth Smart", IEEE Consumer Electronics Mag., 2014

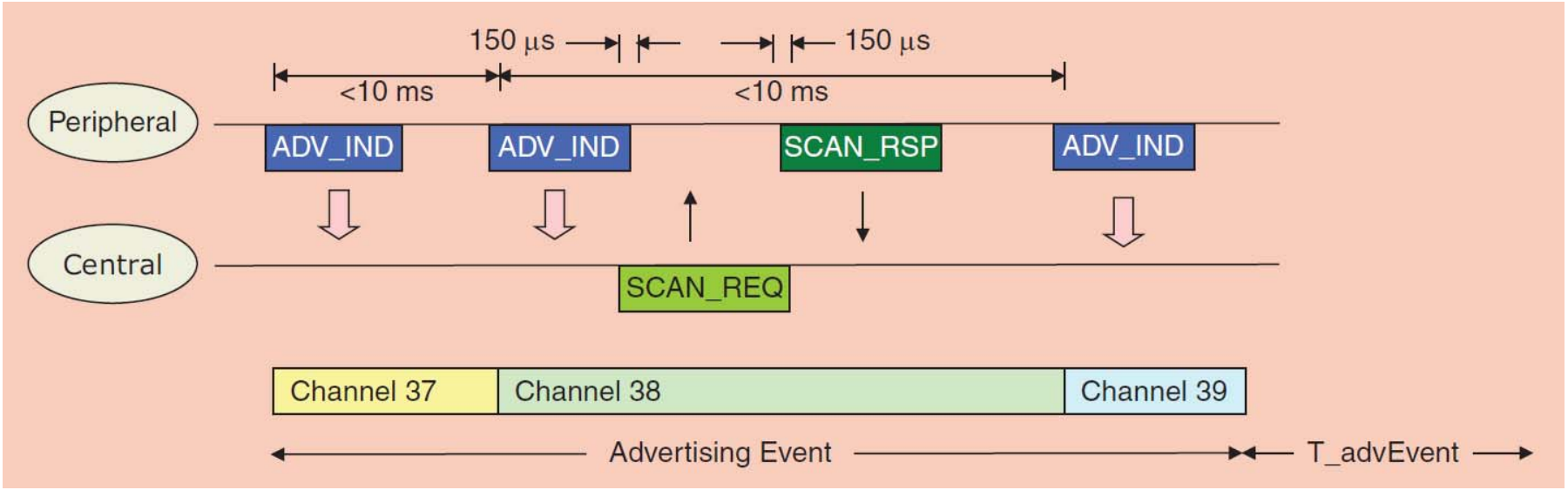
Bluetooth Smart – Advertising

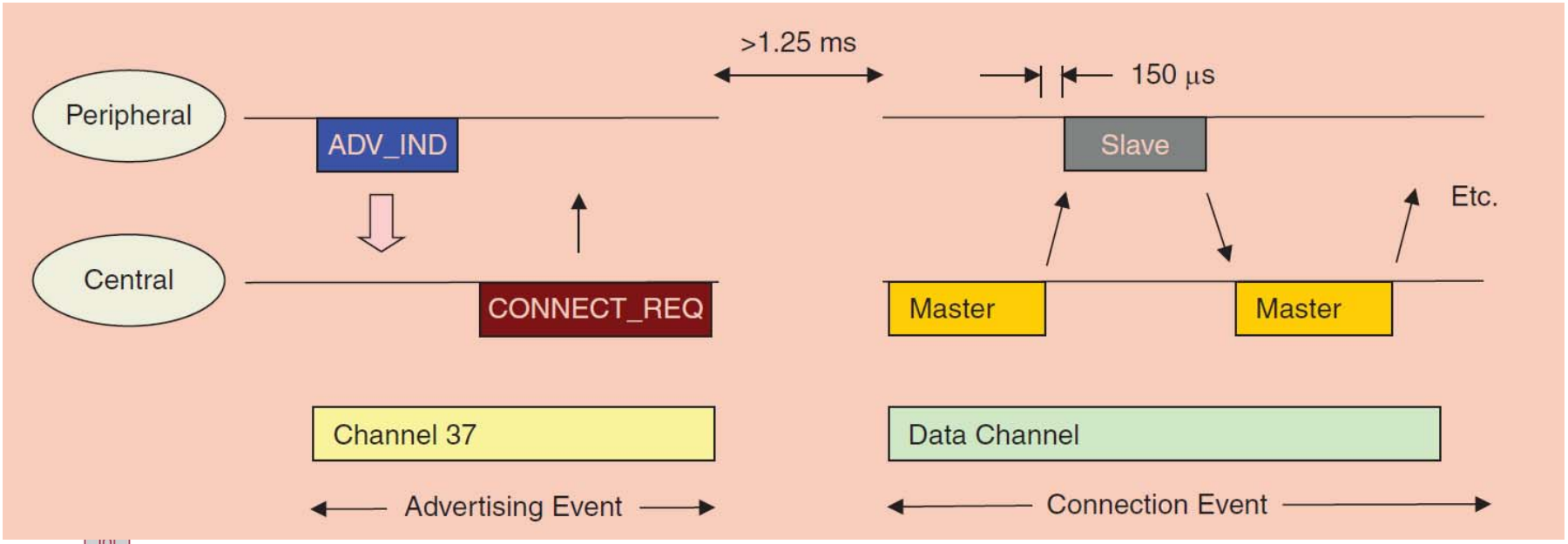


Source: J. Decuir: „Introducing Bluetooth Smart", IEEE Consumer Electronics Mag.

- **3 channels** are set aside for device discovery
  - chosen to avoid the most common Wi-Fi channels in the 2.4-GHz ISM band
- advertiser sends out advertising packets in series
- devices can advertise for various reasons, including:
  - to broadcast promiscuously
  - to transmit signed data to a previously bonded device
  - to advertise their presence to a device wanting to connect
  - to reconnect asynchronously due to a local event
  - to act as a location beacon.

Bluetooth Smart – Data Transactions





Source: J. Decuir: „Introducing Bluetooth Smart", IEEE Consumer Electronics Mag., 2014