Wireless Sensor Networks - ZigBee

Anneleen Van Nieuwenhuyse

KaHo Sint-Lieven – DraMCo – 21/05/2009

Overview

- Introduction
- Wireless Sensor Networks (General)
- IEEE 802.15.4
  - Physical Layer
  - Medium Access Control Layer
- ZigBee
  - Network Layer
  - Application Layer

Introduction

Anneleen Van Nieuwenhuyse
KaHo Sint-Lieven – DraMCo – 21/05/2009

Introduction

- KaHo St – Lieven
- DraMCo
- ECUMICT

KaHo St – Lieven

- Catholic University College Ghent, Belgium
- Department of Electronics / ICT Engineering

Research group: DraMCo

DraMCo

research group

Wireless and Mobile Communication

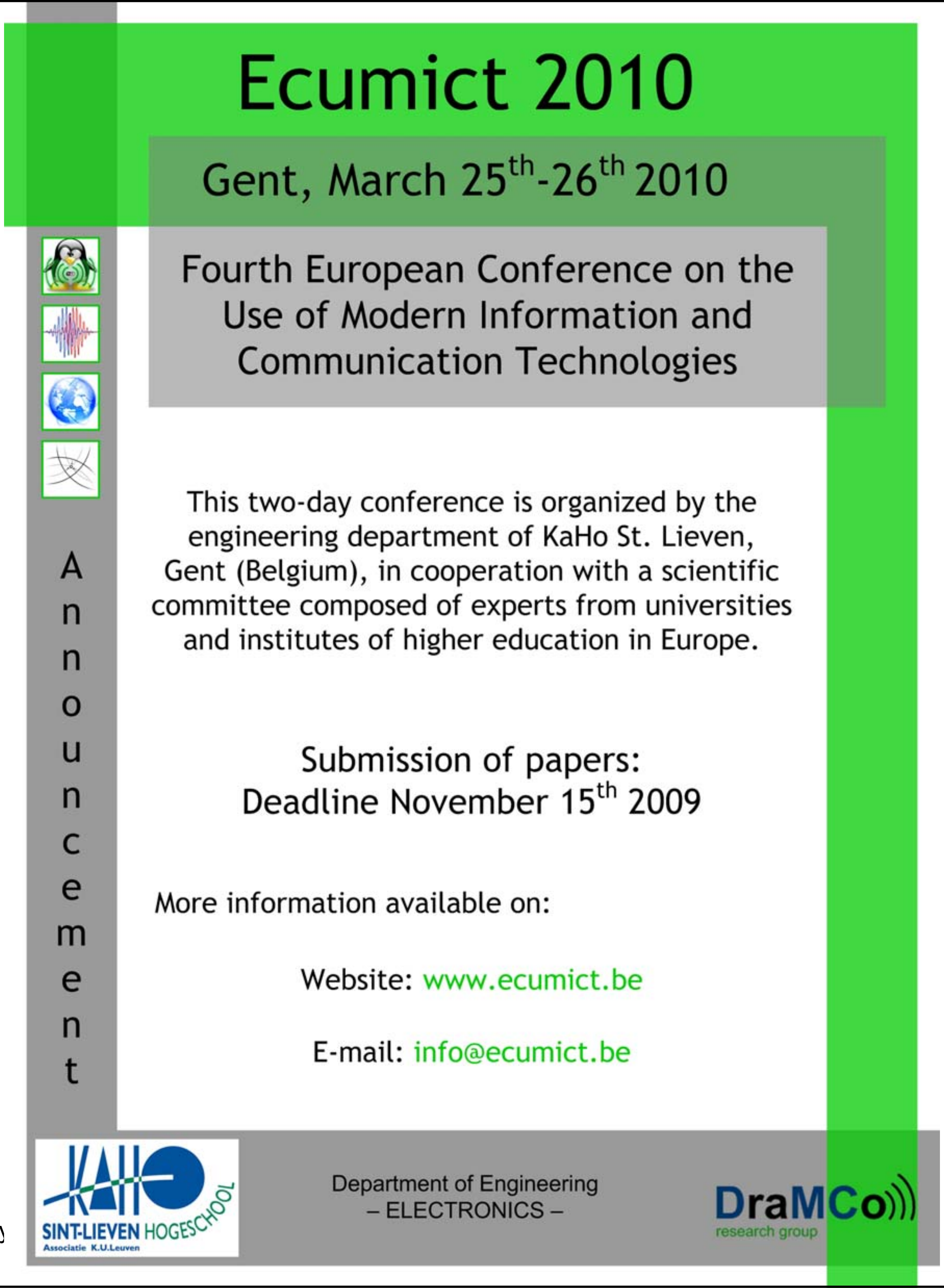
- study of standards and systems for wireless and mobile communication
- Projects:
  - Indoor localization using ZigBee
  - RFID: Used for detection of elderly people in rest houses
  - RFID: Used in automotive sector to track goods

ECUMICT

- **ECUMICT**

  European Conference on the Use of Modern Information and Communication Technologies
- **4th Edition, March 25th - 26th 2010, Ghent**
- **www.ecumict.be**
- **Some themes:**
  - **Applications of Digital Signal Processing**
  - **Speech and image processing**
  - **Multimedia Communication Systems**
  - **Telecommunication Networks and Services**
  - **The use of ICT for educational purposes, including E-learning**
  - **Optimisation techniques in electronic design**
  - **Application development for mobile devices**

ECUMICT



Ecumict 2010

Gent, March 25th-26th 2010

Fourth European Conference on the Use of Modern Information and Communication Technologies

Announcement

This two-day conference is organized by the engineering department of KaHo St. Lieven, Gent (Belgium), in cooperation with a scientific committee composed of experts from universities and institutes of higher education in Europe.

Submission of papers:
Deadline November 15th 2009

More information available on:

Website: www.ecumict.be

E-mail: info@ecumict.be

Department of Engineering
– ELECTRONICS –

ZigBee – Wireless Sensor Networks

Anneleen Van Nieuwenhuyse
KaHo Sint-Lieven – DraMCo – 21/05/2009

Overview

- Wireless Sensor Networks
  - What are wireless sensor networks?
  - Application examples
  - Challenges
  - Architecture of sensor nodes
  - Examples of sensor nodes
- Introduction to ZigBee
  - Introduction
  - IEEE 802.15.4 / ZigBee protocol stack
  - Network Topologies
  - Network components
  - ZigBee Architecture

Wireless Sensor Networks

KaHo Sint-Lieven – DraMCo – 21/05/2009

What are wireless sensor networks?

- Many devices spread over a large space or area
- All devices form 1 large network
- Sensors on devices to measure / guard environmental conditions
  - Temperature sensors
  - Sound sensors
  - Vibration sensors
  - Light sensors
  - …
- Capacities of nodes have constraints
  - Energy provision
  - Memory
  - Transmission range
  - Calculation Capacity

=> Co-operate

Application Examples

- Intelligent Buildings
  - Equip buildings with sensors so the energy cost can be reduced
- Health care
  - Monitor the health condition of patients by the use of sensor nodes
  - Wireless communication => less physical restriction
- Logistics
  - Connect sensors on packages or containers
  - Track goods during transport / in the warehouse
- Precision agriculture
  - Precision-irrigation
  - Humidity sensors
  - Large network with low density

Challenges

- Characteristics of WSN’s
  - Quality of Service (QoS):
    - Different applications have different requirements concerning the delivered quality
    - ~ delivering all packets
    - ~ delivering the packets on time
    - Ex: Temperature measurement in a building vs. power plant
  - Fault tolerance:
    - Nodes can drop out of the network
    - Automatic reconfiguration of the network
  - Lifetime
    - Restricted energy available for each node
    - Autonomy of a device has to be as large as possible
    - Introduction of several operational modes
    - Decreasing energy consumption => decreasing QoS

Challenges

- Characteristics of WSN’s
  - Scalability
    - Possibly thousands of nodes for each network
    - Protocol must be able to deal with that
      - Useful routing mechanism
      - Complete coverage of the network, to be able to reach all nodes
      - Fault tolerance
    - Ex: Detection of forest fires
  - Wide range of densities
    - Different applications require different densities of the spreading of the nodes
    - Ex: Agriculture vs. Health care

Challenges

- Mechanisms in WSN
  - Multi-hop wireless communication
    - Restricted energy available
    - Restricted transmission range
    - Transmit data through multi-hop communication
  - Energy-efficient functioning
    - Enlarge the autonomy of devices
    - Introduce different operation modes
  - Auto-configuration
    - Allow nodes at start-up to form their own network
    - Detection of nodes in the neighbourhood / within the transmission range
    - Reconfiguration of the network when nodes drop out
  - Co-operation
    - Restricted capacities for each node
    - Make co-operation between different nodes possible
    - Ex: Detection of room temperature

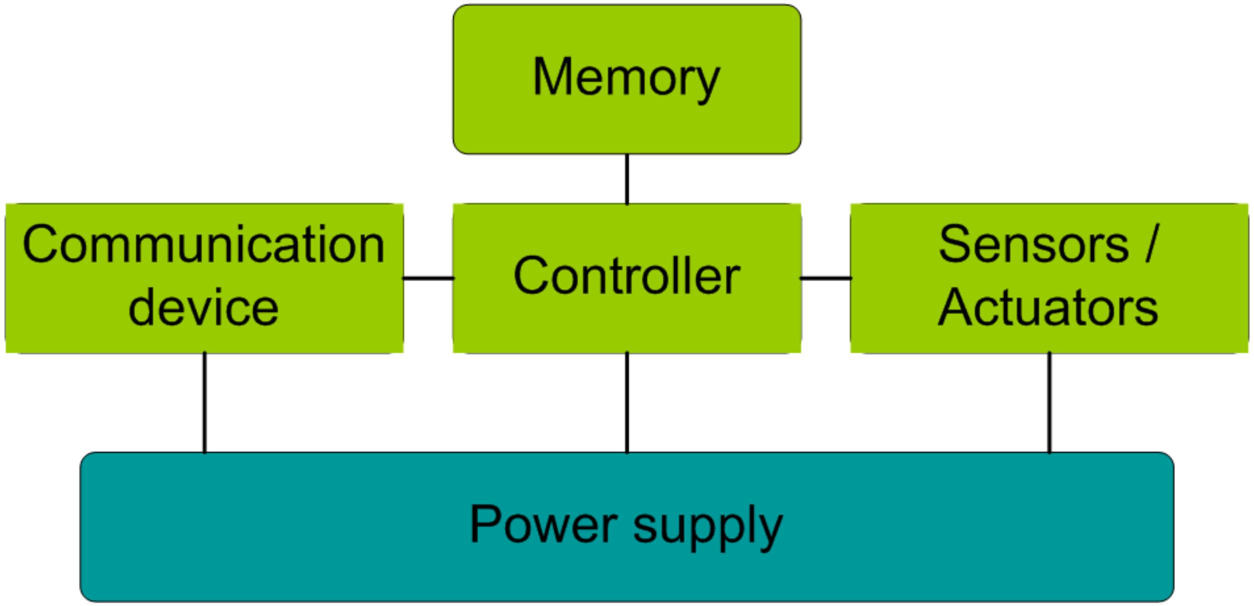
Architecture of sensor nodes

- Most important tasks of sensor nodes:
  - Communication
  - Perform measurements (sensing)
  - Perform calculations
  - Storage of data
- Hardware of sensor nodes:
  - Cost
  - Size
  - Energy consumption
  - Calculation capacity

  ⇒ Application dependent

Architecture of sensor nodes

- Hardware components of sensor nodes:



Architecture of sensor nodes

- Controller
  - In connection with all other components
  - Collect sensor data
  - Process data
  - Take decisions
- Memory
  - RAM (Random Access Memory)
    - Store intermediate collected measurements
    - Store received packets
  - ROM (Read-Only Memory)
    - Program code

Architecture of sensor nodes

- Sensors
  - Passive omni-directional sensors
  - Passive smallband sensors
  - Active sensors
- Communication
  - Data exchange between different nodes
  - Radio Frequency
  - Pick out suitable transceiver
    - Energy-efficiency
    - Carrier frequency
    - Gain
    - Sensitivity of receiver

Architecture of sensor nodes

- Power supply
  - Nodes often positioned on unreachable places
  - Many many nodes

  ⇒ Battery-power

Architecture of sensor nodes

- Energy consumption:
  - Battery-power
  - Controller, transceiver, memory and sensors use many energy
  - A node does not work during large amount of the time

  ⇒ Different operational modes: Power down the energy users

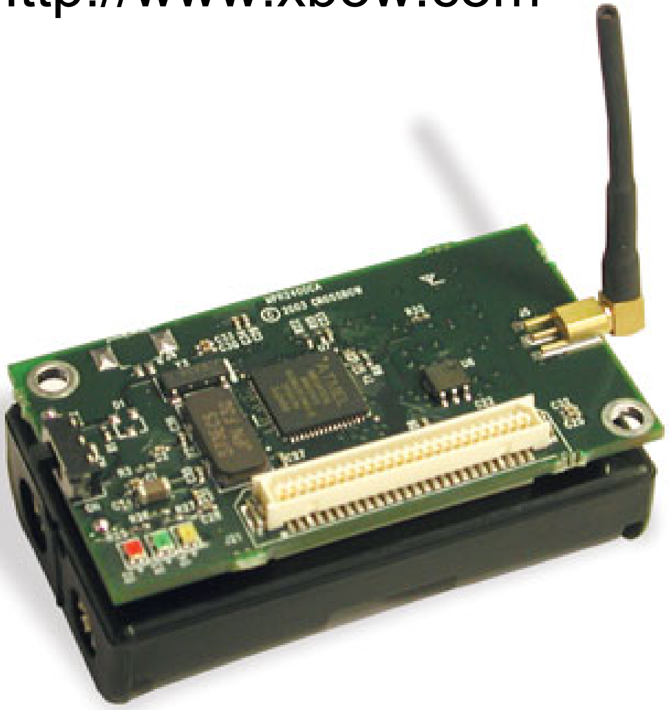
  ⇒ Energy consumption decreases and leads to decreasing functionality

  - Active
  - Idle
  - Sleep

  ⇒ The deeper a node is sleeping, the more energy it costs to switch to the active mode

Examples of sensor nodes

- ‘Mica Mote’ family
  - Low-power WSN
  - Frequency 2.4 GHz
  - Compatible with IEEE 802.15.4
  - TinyOS Operating System
  - University of California Berkeley
  - Manufacturer Crossbow
  - Mica, Mica2, Mica2Dot
  - Http://www.xbow.com



Examples of sensor nodes

- EYES node (Energy Efficient Sensor Networks)
- European project, European universities
- Goal van sensor network:
  - self-organizing
  - self-reconfigurable
  - energy-efficient
  - autonomous
- http://www.eyes.eu.org/

Examples of sensor nodes

- BT node
  - Microcontroller: Atmel ATmega 128L (8 MHz @ 8 MIPS)
  - Memory: 64+180 kByte RAM, 128 kByte FLASH ROM, 4 kByte EEPROM
  - Bluetooth radio
  - Low-power radio: Chipcon CC1000 operating in ISM band 433-915 MHz
  - Extern Interfaces: ISP, UART, SPI, ADC, Timer, 4 LED’s
  - TinyOS compatible
  - http://www.btnode.ethz.ch

Introduction to ZigBee

KaHo Sint-Lieven – DraMCo – 21/05/2009

Introduction

- ZigBee was developed for Wireless Personal Area Networks (WPAN's)
- ZigBee Alliance (http://www.zigbee.org)

ZigBee® Alliance

- Properties of ZigBee networks:
  - Low-power
  - Low-cost
  - Low-data rate
  - Self-healing
  - Self-forming

WPAN ?

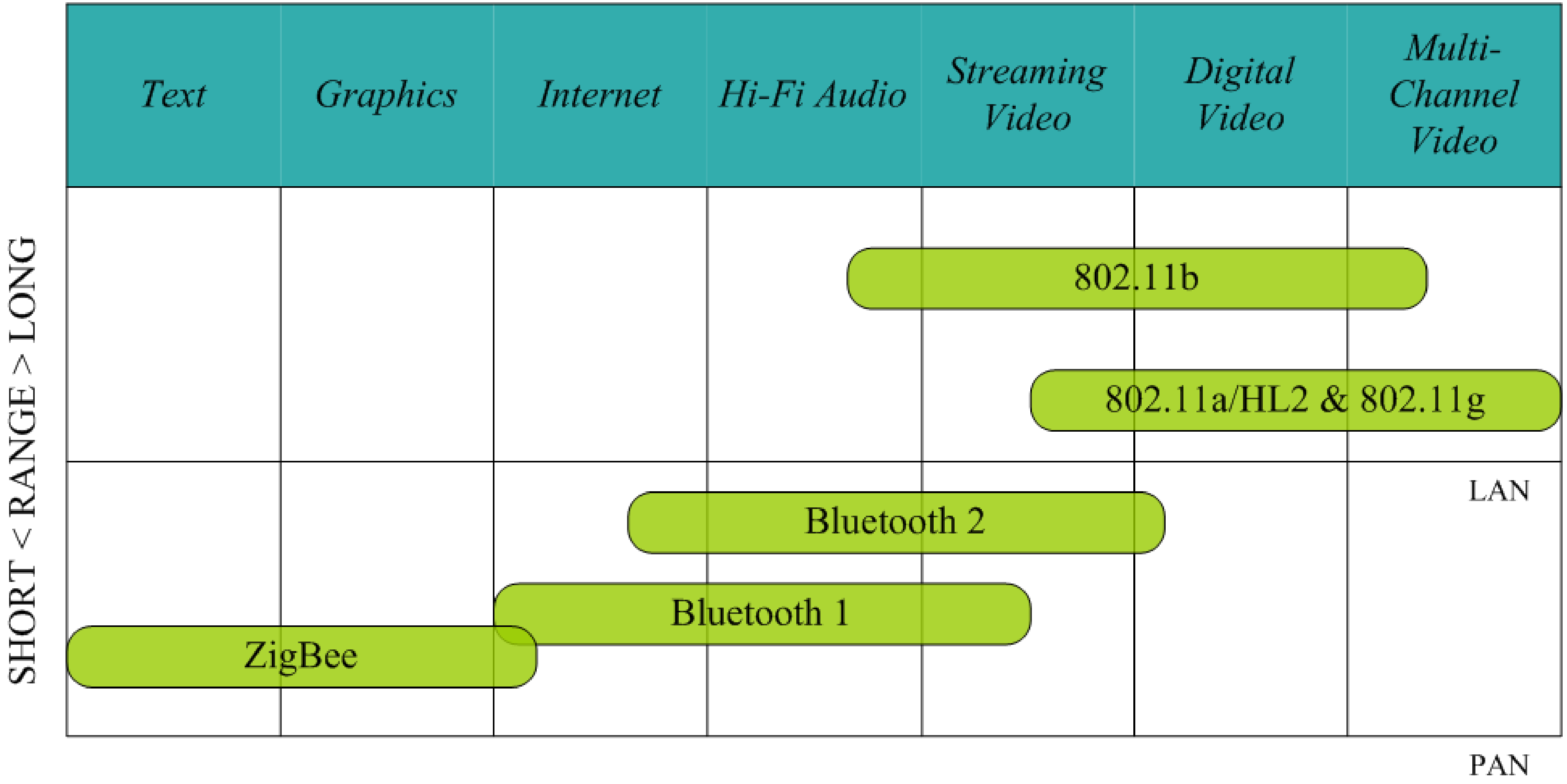
- WPAN : Wireless Personal Area Networks
- short distance wireless networks
- Definition: wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, consumer electronics, sensors, etc; allowing these devices to communicate and interoperate with one another.
- Ranging
  - from point-to-point to meshed networks containing thousands of node
  - from low bit rate to high bit rate
  - from low connection rate to high connection rate

⇒ various applications with different requirements

⇒ different standards, with flexibility in standards

Introduction

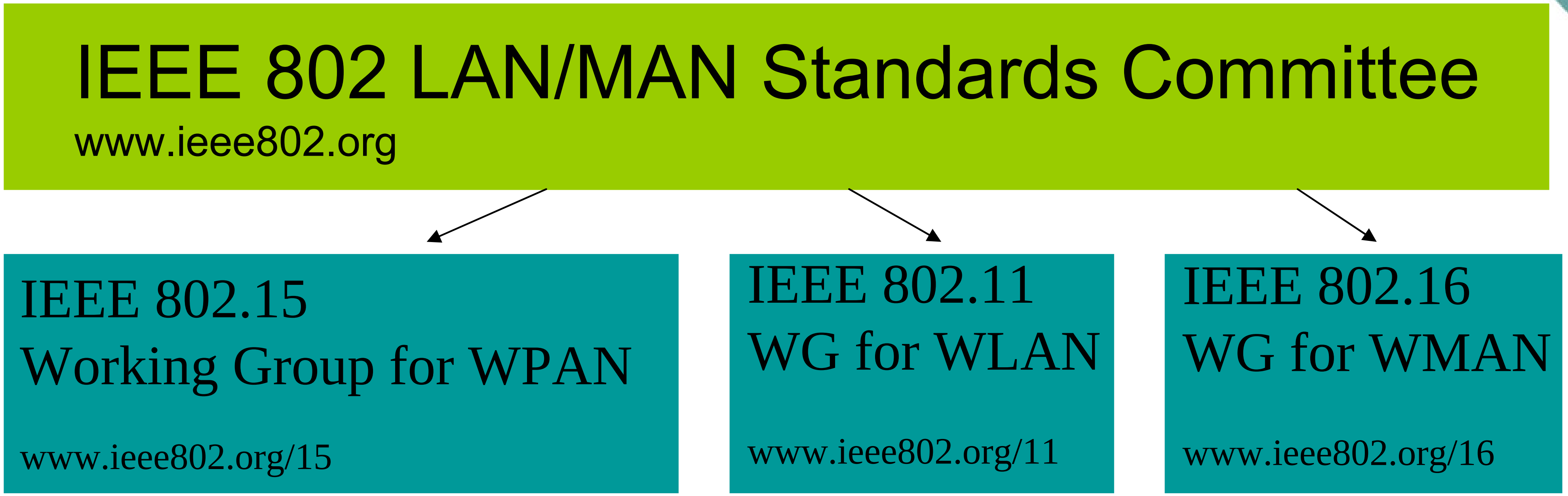
- Comparison with other wireless technologies



WPAN

- Open standards based on IEEE standards
  - High rate
  - Medium rate : Bluetooth
  - Low rate : ZigBee
- But other technologies exist
  - Z-wave
    - proprietary (Zensys, Denmark): protocol for home control
    - Z-wave Allience : 14/1/2005 http://www.z-wavealliance.com/
    - 868.42 MHz; BFSK ± 20 kHz; 9600 bits/s
    - Meshed networks (≤232 nodes), routing along different nodes, two-way with ack
  - X10
    - Powerline protocol first introduced in the 1970's.
    - http://www.x10.com/technology1.htm
  - IO Homecontrol
  - INSTEON
    - Peer-to-peer mesh networking product that features a hybrid radio/powerline transmission
    - http://www.insteon.net
  - nanoNET
    - Proprietary set of wireless sensor protocols, designed to compete with ZigBee.
    - http://www.nanotron.com/

Who’s standardizing what ?



IEEE 802 LAN/MAN Standards Committee

www.ieee802.org

IEEE 802.15
Working Group for WPAN

www.ieee802.org/15

IEEE 802.11
WG for WLAN

www.ieee802.org/11

IEEE 802.16
WG for WMAN

www.ieee802.org/16

IEEE 802.15.1 Medium rate WPAN
Bluetooth v1.1 PHY + MAC
IEEE 802.15.3 High rate WPAN
IEEE 802.15.4 Low Rate WPAN
ZigBee PHY + MAC
IEEE 802.15.6 BAN

WiFi

WiMax

Who’s standardizing what ?

Bluetooth

Bluetooth SIG
www.bluetooth.org

Higher layers

IEEE 802.15.1

PHY + MAC

ZigBee™

ZigBee Alliance
www.zigbee.org

Higher layers

IEEE 802.15.4

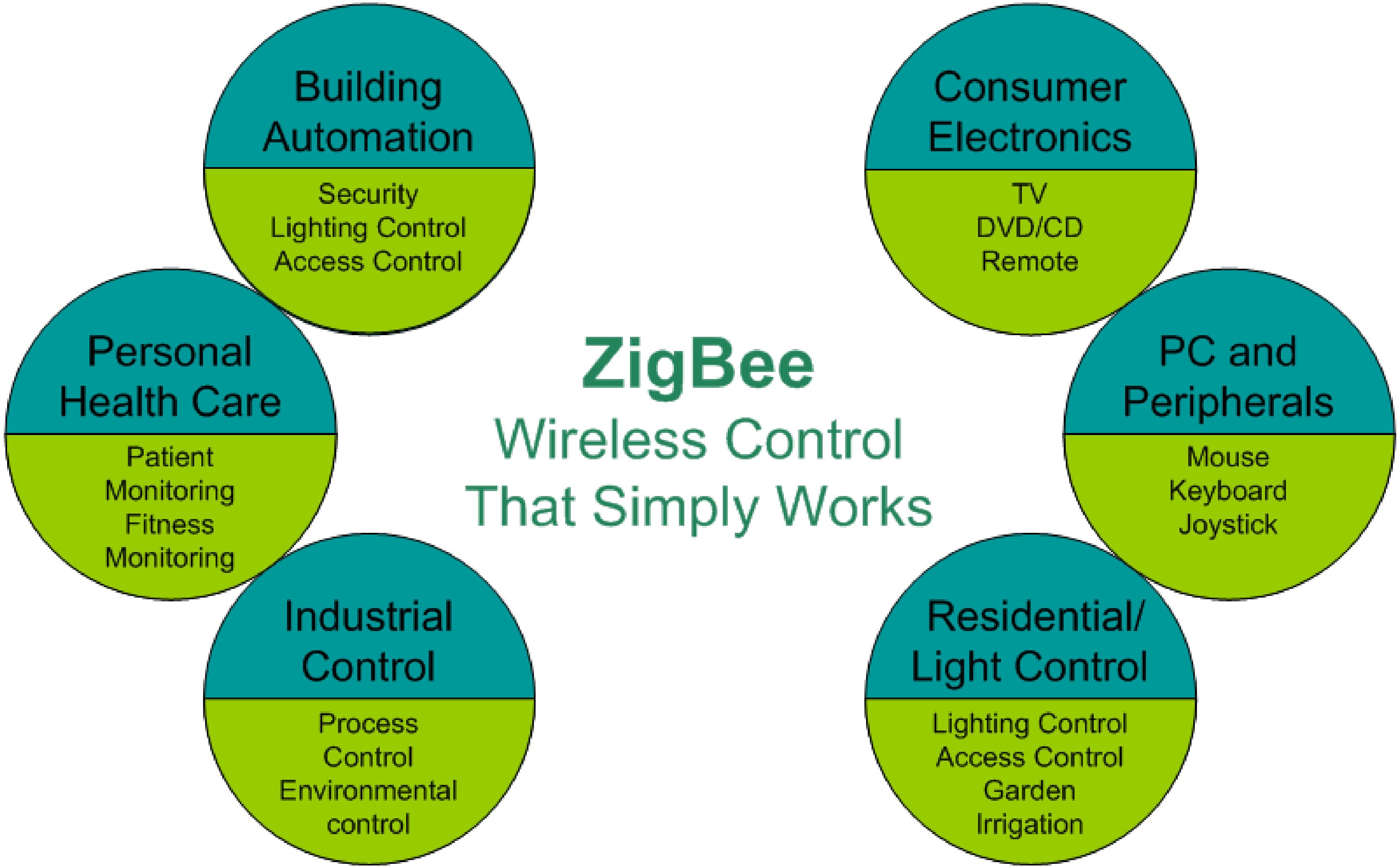
PHY + MAC

Introduction

- Properties of ZigBee networks:
  - Low-power
  - Low-cost
  - Low-data rate
  - Self-healing
  - Self-forming

Introduction

- Application field of ZigBee



Building Automation
Security
Lighting Control
Access Control

Consumer Electronics
TV
DVD/CD
Remote

Personal Health Care
Patient Monitoring
Fitness Monitoring

PC and Peripherals
Mouse
Keyboard
Joystick

Industrial Control
Process Control
Environmental control

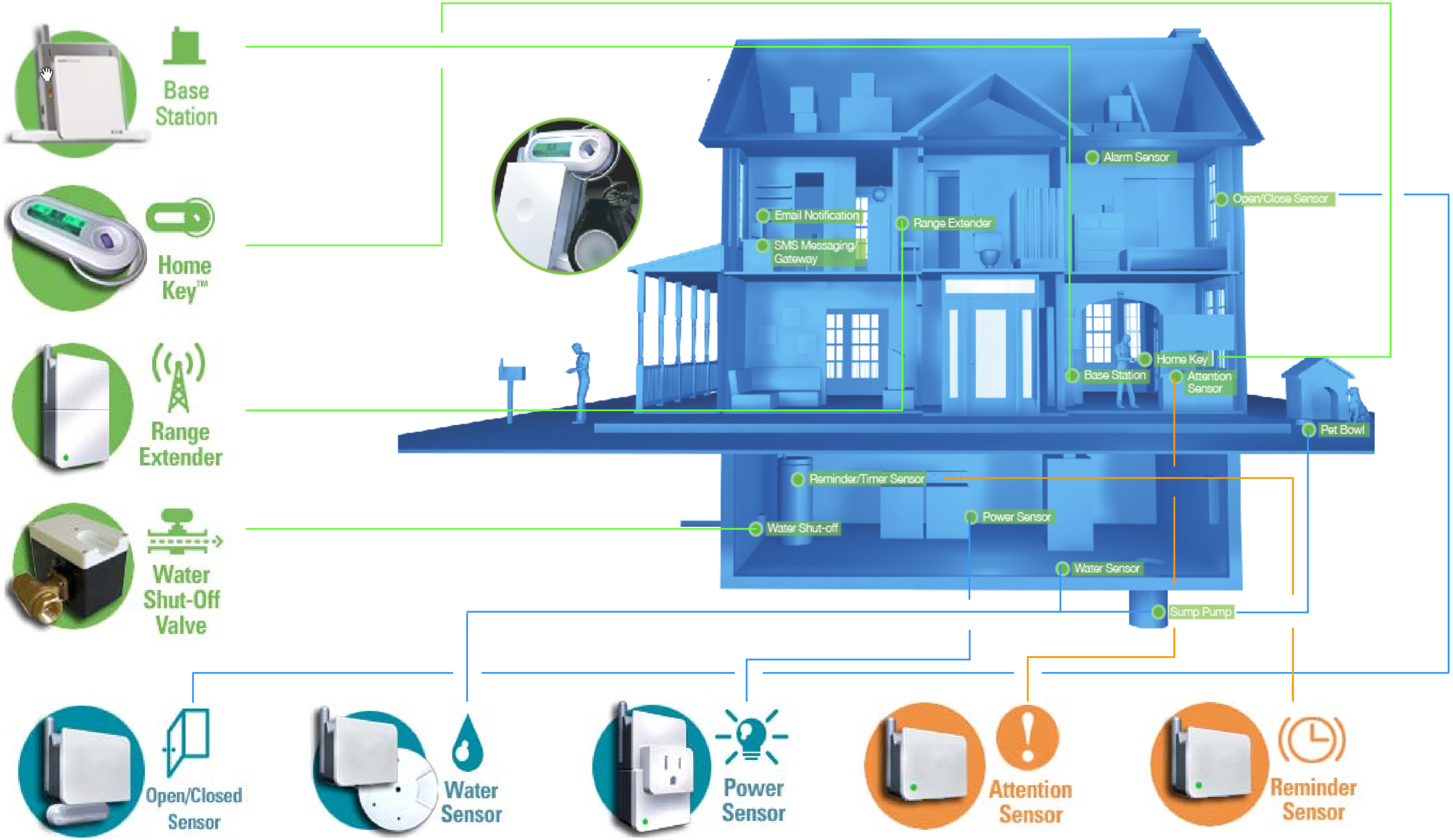
Residential/ Light Control
Lighting Control
Access Control
Garden Irrigation

ZigBee
Wireless Control That Simply Works

Introduction: Examples

Home Heartbeat

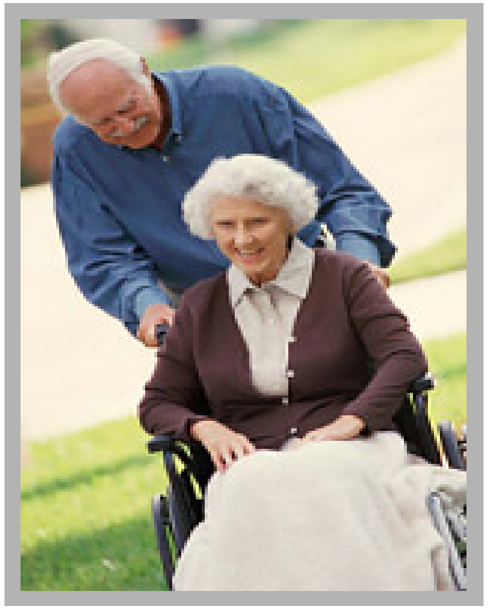
EATON



Introduction: Examples

Introduction: Examples

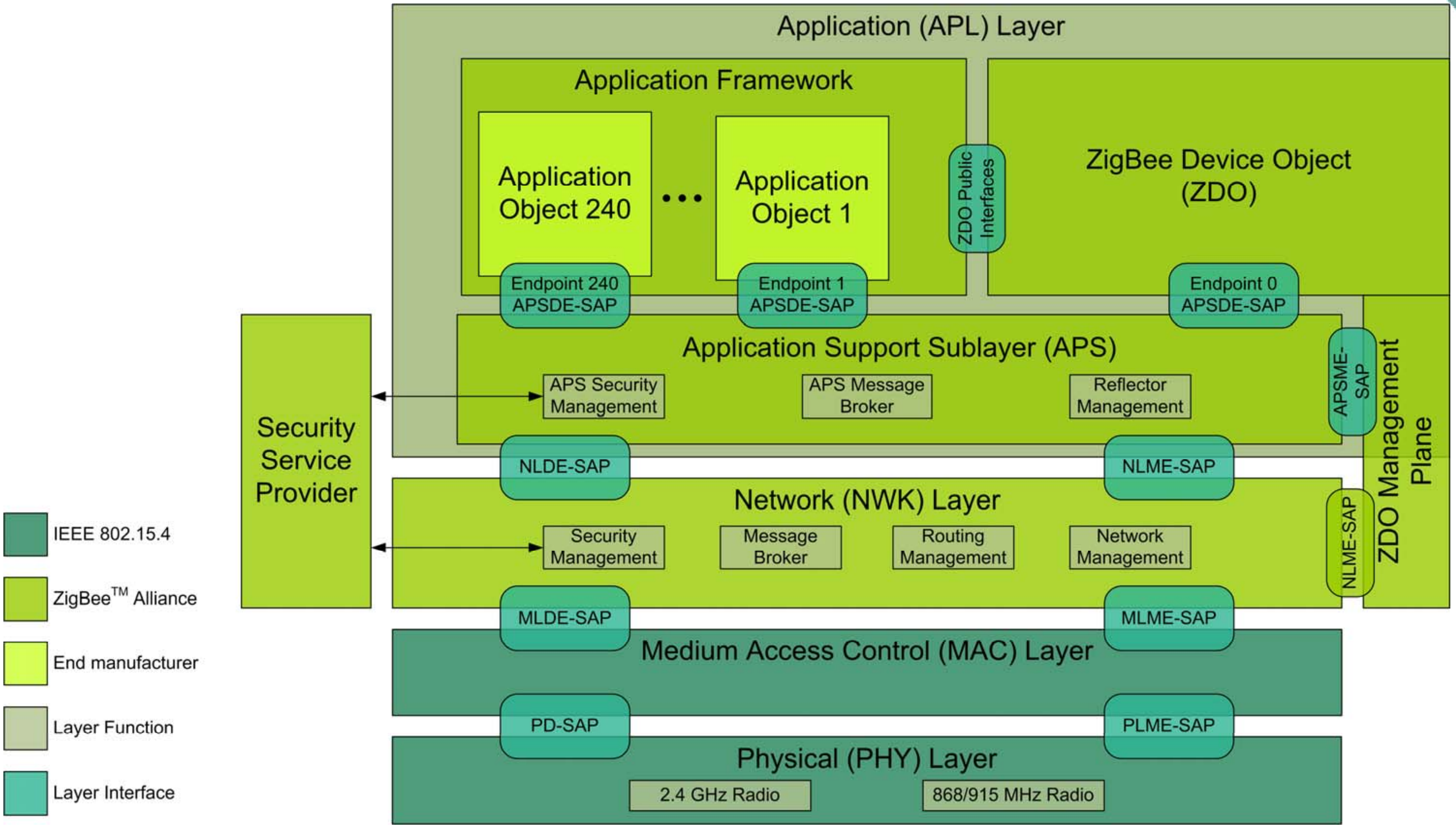
- Applications In-Home Patient Monitoring
- Patients receive better care at reduced cost with more freedom and comfort---
  - Patients can remain in their own home
    - Monitors vital statistics and sends via internet
    - Doctors can adjust medication levels
  - Allows monitoring of elderly family member
    - Sense movement or usage patterns in a home
    - Turns lights on when they get out of bed
    - Notify via mobile phone when anomalies occur
    - Wireless panic buttons for falls or other problems
  - Can also be used in hospital care
    - Patients are allowed greater movement
    - Reduced staff to patient ratio



Introduction: Examples

- Hotel energy management
  - Centralized HVAC management allow hotel operator to ensure empty rooms are not cooled
  - Easy to retrofit
  - Battery operated thermostats, occupancy detectors, humidistats can be placed for convenience
  - Personalized room settings at check-in

IEEE 802.15.4 / ZigBee protocol stack



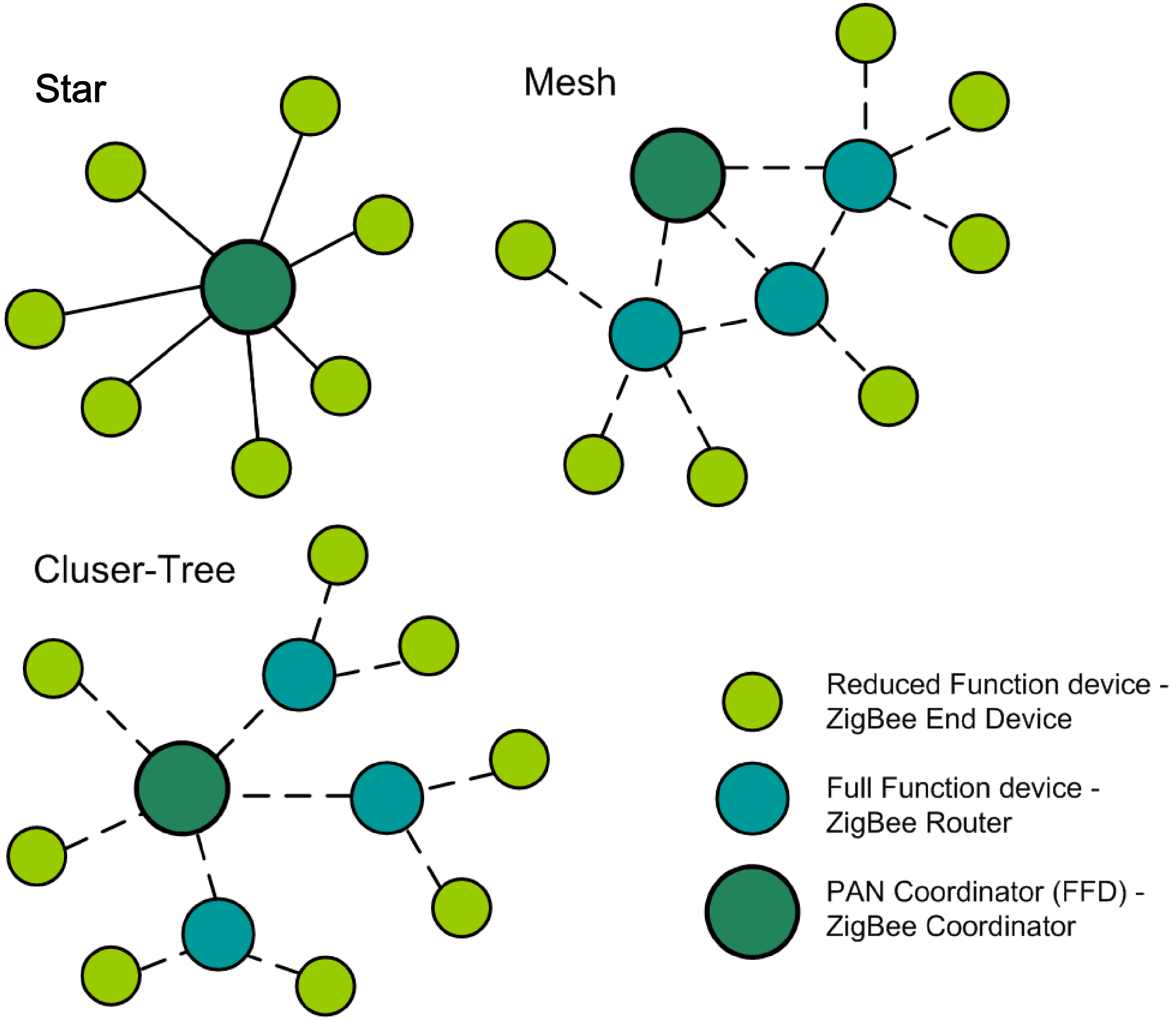
IEEE 802.15.4 / ZigBee protocol stack : IEEE 802.15.4

- IEEE 802.15.4:
  - Defines physical layer (PHY) and media access control layer (MAC)
  - Low-Rate Wireless Personal Area Networks (LR-WPAN’s)
  - Focuses on low-cost, low-speed communication between devices
- PHY: Hardware for wireless transmission of data
  - Determine type of RF transmitter/receiver
  - Select frequency and channel for transmission
  - Chose modulation technique
- MAC: Transmission and reception of data through the PHY
  - Beacon management
  - Channel access
  - Synchronisation
  - Association / dissociation of devices

IEEE 802.15.4 / ZigBee protocol stack : ZigBee

- ZigBee:
  - Defines the Network Layer (NWK) and the Application layer (APL)
  - Focuses on low data rate, large autonomy and elaboration of safe networks
- NWK: Network management
  - Allow devices to join and leave the network
  - Assign network addresses
  - Calculate and discover routes throughout the network
- APL: Support the applications of the end-user
  - Application Support Sub-layer (APS)
  - Application Framework (AF)
  - ZigBee Device Object (ZDO)

Network topologies



● Reduced Function device - ZigBee End Device

● Full Function device - ZigBee Router

● PAN Coordinator (FFD) - ZigBee Coordinator

Network Components

- IEEE 802.15.4 standard defines 2 types:
  - Full Function Device (FFD)
    - Communicates with FFD’s en RFD’s
    - Performs the synchronisation by sending beacons
  - Reduced Function Device (RFD)
    - Communicates only with FFD
    - Reduced functionality
    - Device does not send beacons
- Each network has at minimum 1 FFD = PAN Co-ordinator

ZigBee Architecture

- ZigBee standard defines 3 types:
  - ZigBee Co-ordinator (ZC)
    - One ZC present at each network = IEEE 802.15.4 PAN Co-ordinator (FFD)
    - Initialises the network
    - Router once the network is formed
  - ZigBee Router (ZR)
    - Associates to a ZC or ZR
    - Elaboration of the network
    - Assigns addresses locally
    - Helps with the routing of messages
    - Acts as an IEEE 802.15.4 Co-ordinator (FFD)
  - ZigBee End Device (ZED)
    - Associates to a ZC or ZR
    - Other devices can not associate to ZED's
    - No routing of messages
    - Act as an IEEE 802.15.4 RFD

ZigBee – Physical Layer

Anneleen Van Nieuwenhuyse
KaHo Sint-Lieven - DraMCo – 21/05/2009

Overview

- Introduction
- Frequency bands
- Data transmission
  - modulation : what en why ?
  - physical frame
- Functional description
- Range and indoor radio propagation

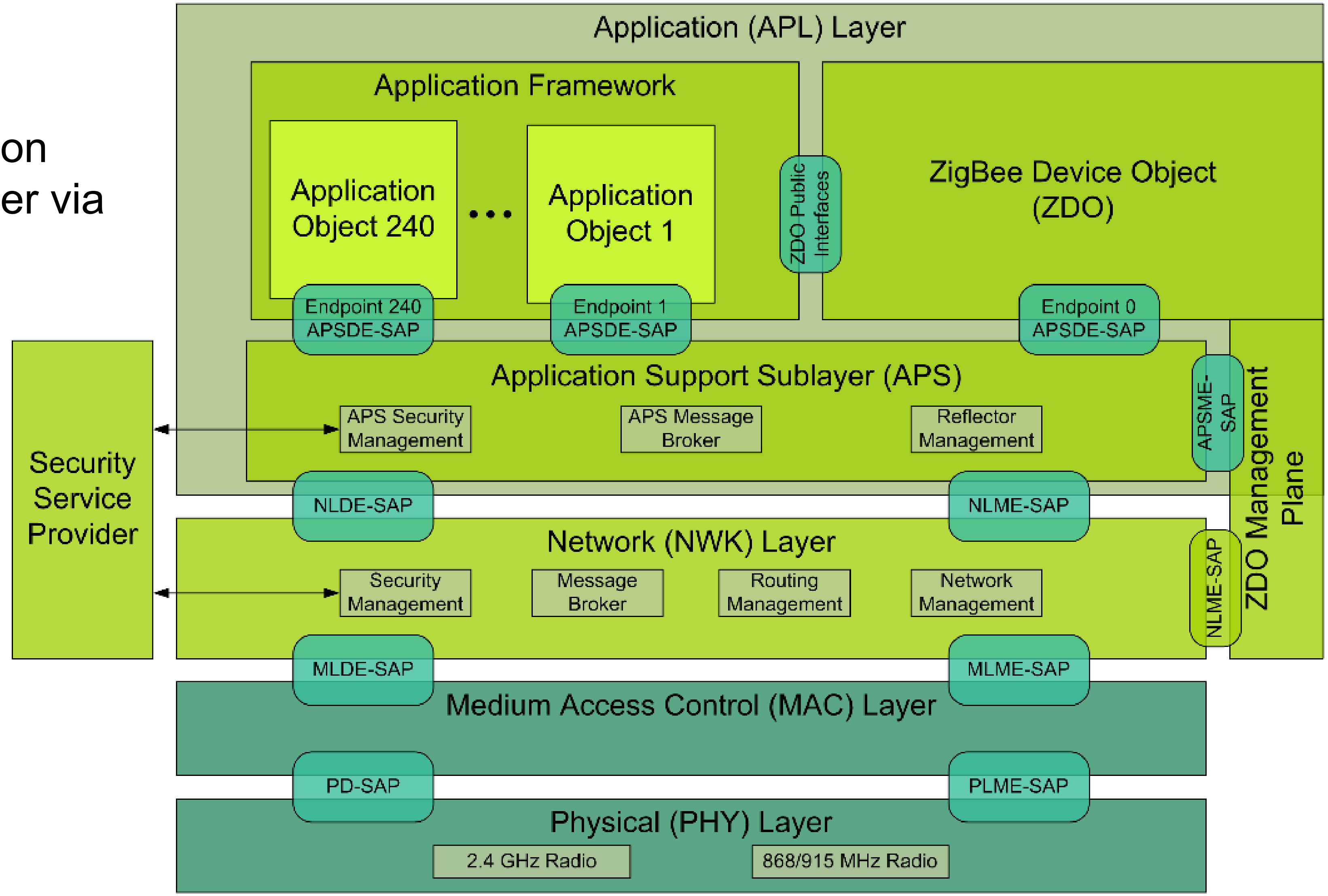
Physical layer

- Physical (hardware) aspects of the transmission

- Frequency
- Transmission power
- Modulation
- Link Quality Indication (LQI)
- Channel selection
- ...

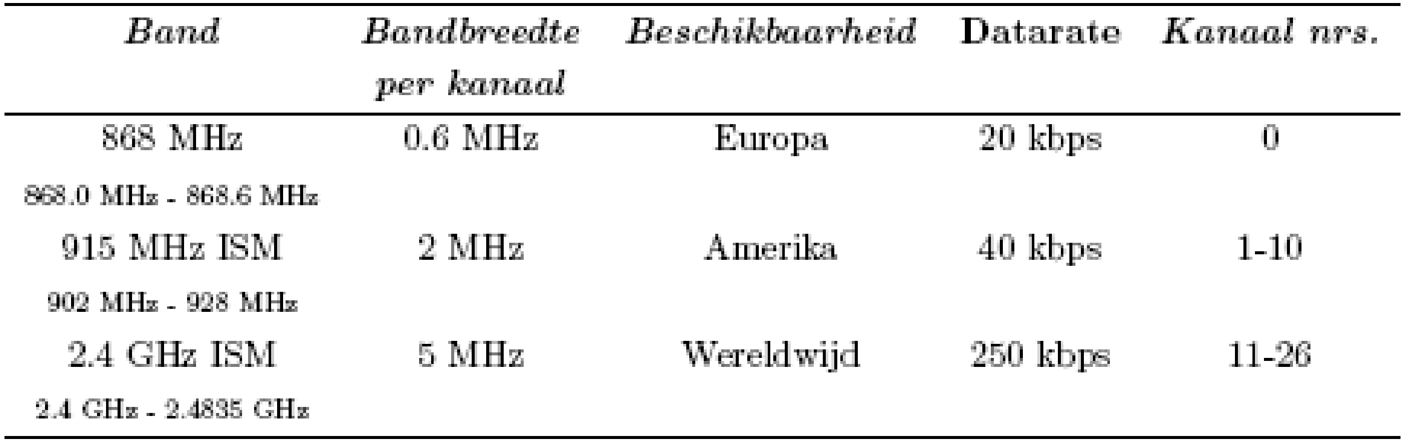
ZigBee Protocol stack

Communication with MAC layer via SAP's

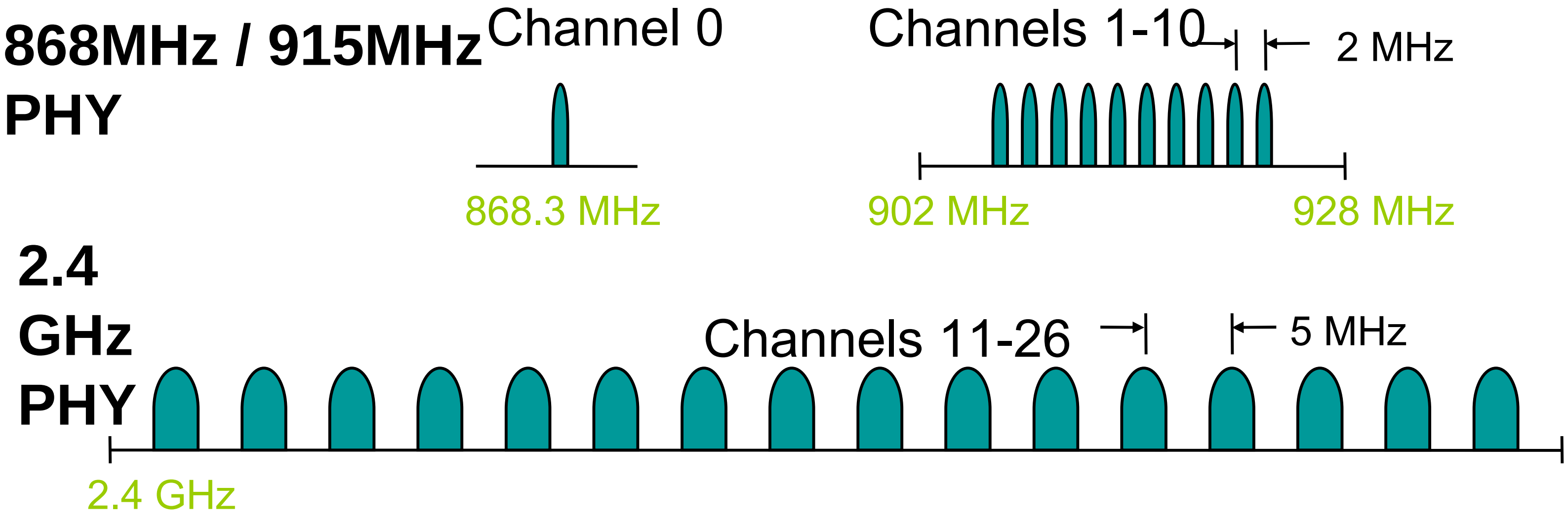


- 🟩 IEEE 802.15.4
- 🟩 ZigBee^{TM} Alliance
- 🟩 End manufacturer
- 🟩 Layer Function
- 🟩 Layer Interface

Frequency bands



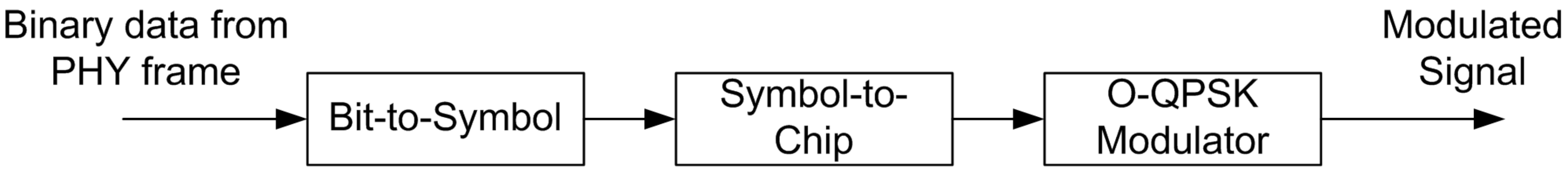
Band	*Bandbreedte per kanaal*	*Beschikbaarheid*	**Datarate**	*Kanaal nrs.*
868 MHz 868.0 MHz - 868.6 MHz	0.6 MHz	Europa	20 kbps	0
915 MHz ISM 902 MHz - 928 MHz	2 MHz	Amerika	40 kbps	1-10
2.4 GHz ISM 2.4 GHz - 2.4835 GHz	5 MHz	Wereldwijd	250 kbps	11-26



Selection of the channel is performed by the co-ordinator (chosen in the higher layers), channel is fixed (ZigBee PRO allows channel hopping)

Modulation

PHY 2.4 GHz

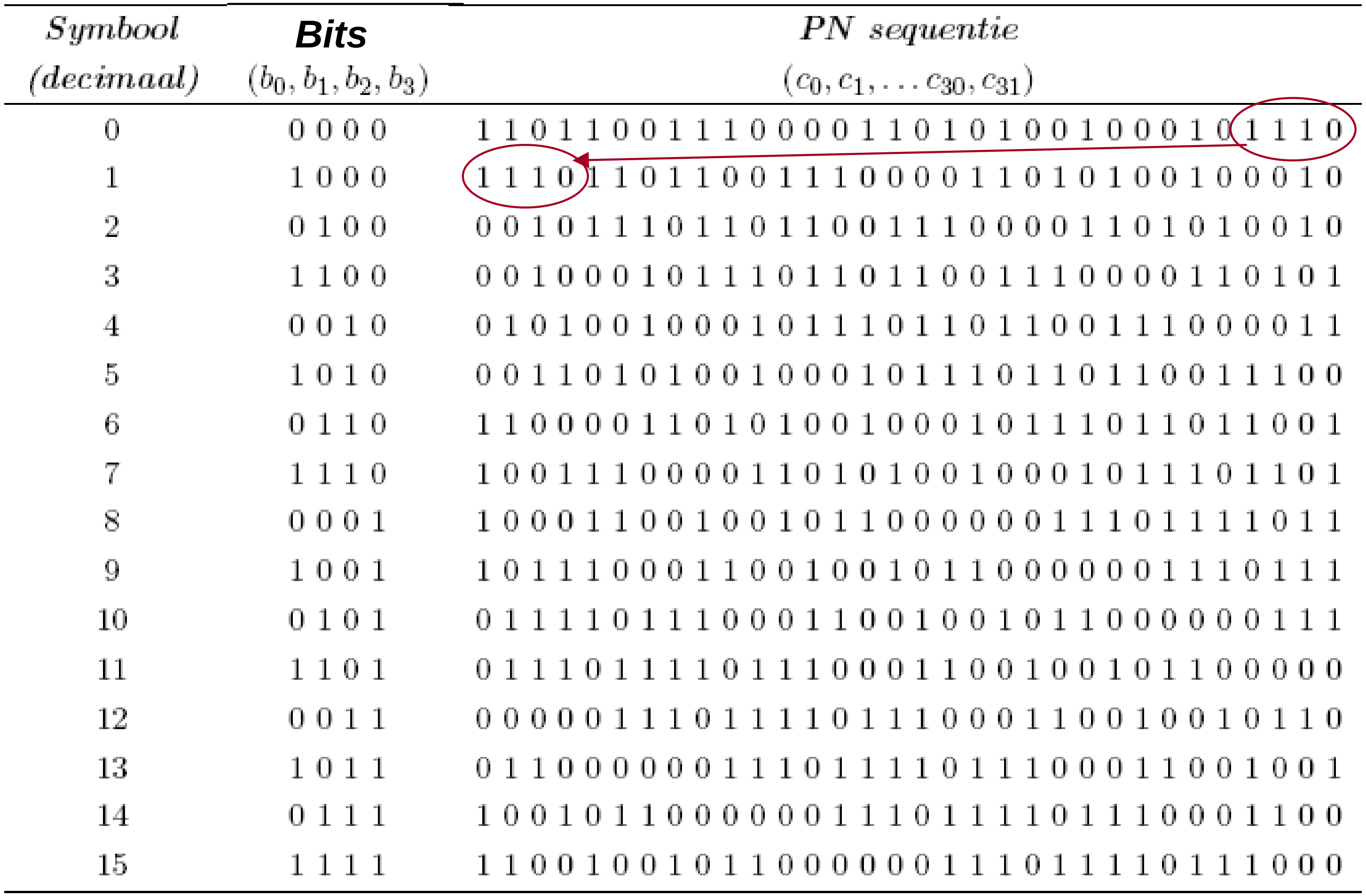


- 250 kb/s (4 bits/symbol, 62.5 kBaud)

- Data modulation is 16-ary orthogonal modulation
- 16 symbols: quasi-orthogonal set of 32-chip Pseudo Noise codes (DSSS)
- Chip modulation is MSK at 2.0 Mchips/s

Modulation

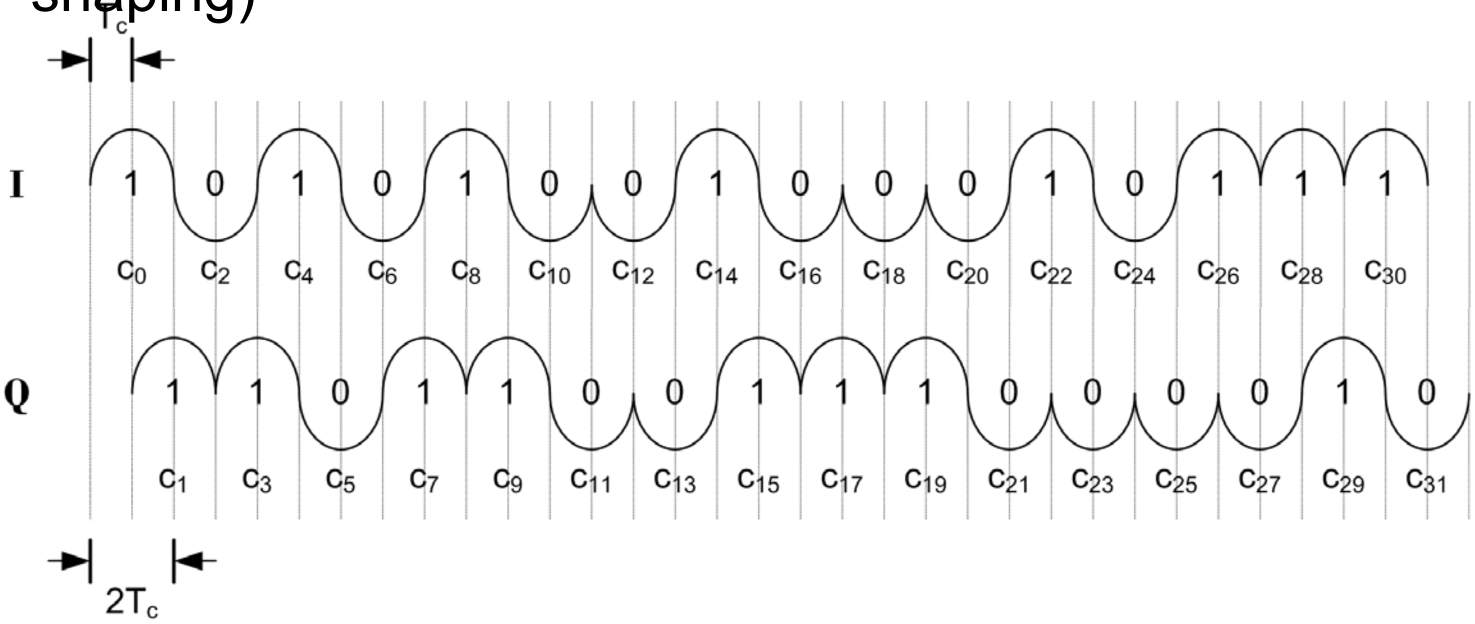
- Bit to Symbol Conversion
- Symbol to Chip Conversion
  - 32 chip PN sequence
  - (0-7) shifted
  - (8-15) odd chips inverted



Symbool *(decimaal)*	**Bits** (b_0, b_1, b_2, b_3)	*PN sequentie* $(c_0, c_1, \ldots c_{30}, c_{31})$
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

Modulation

- Chips are modulated onto a carrier
  - modulation scheme is MSK (= O-QPSK with sinusoidal pulse shaping)


T$_c$
I
1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1
C$_0$ C$_2$ C$_4$ C$_6$ C$_8$ C$_{10}$ C$_{12}$ C$_{14}$ C$_{16}$ C$_{18}$ C$_{20}$ C$_{22}$ C$_{24}$ C$_{26}$ C$_{28}$ C$_{30}$
Q
1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 0
C$_1$ C$_3$ C$_5$ C$_7$ C$_9$ C$_{11}$ C$_{13}$ C$_{15}$ C$_{17}$ C$_{19}$ C$_{21}$ C$_{23}$ C$_{25}$ C$_{27}$ C$_{29}$ C$_{31}$
2T$_c$

$$\begin{aligned} s(t) &= R(t)\cos(\omega_c t + \theta(t)) \\ &= \underset{\underset{\textstyle I}{\uparrow}}{x(t)}\cos\omega_c t - \underset{\underset{\textstyle Q}{\uparrow}}{y(t)}\sin\omega_c t \end{aligned}$$

Modulation

DSSS – MSK : Why go through all this trouble ??

DSSS

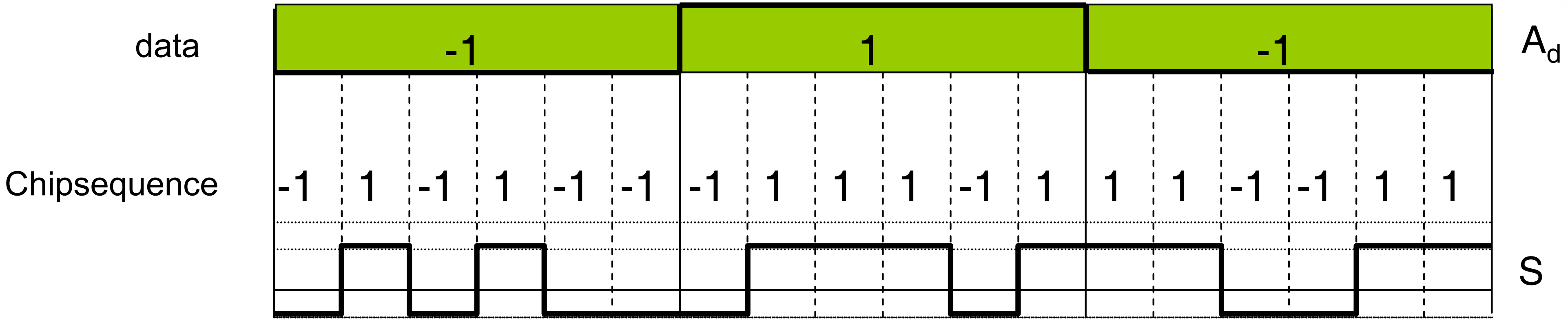
In the time domain

MSK

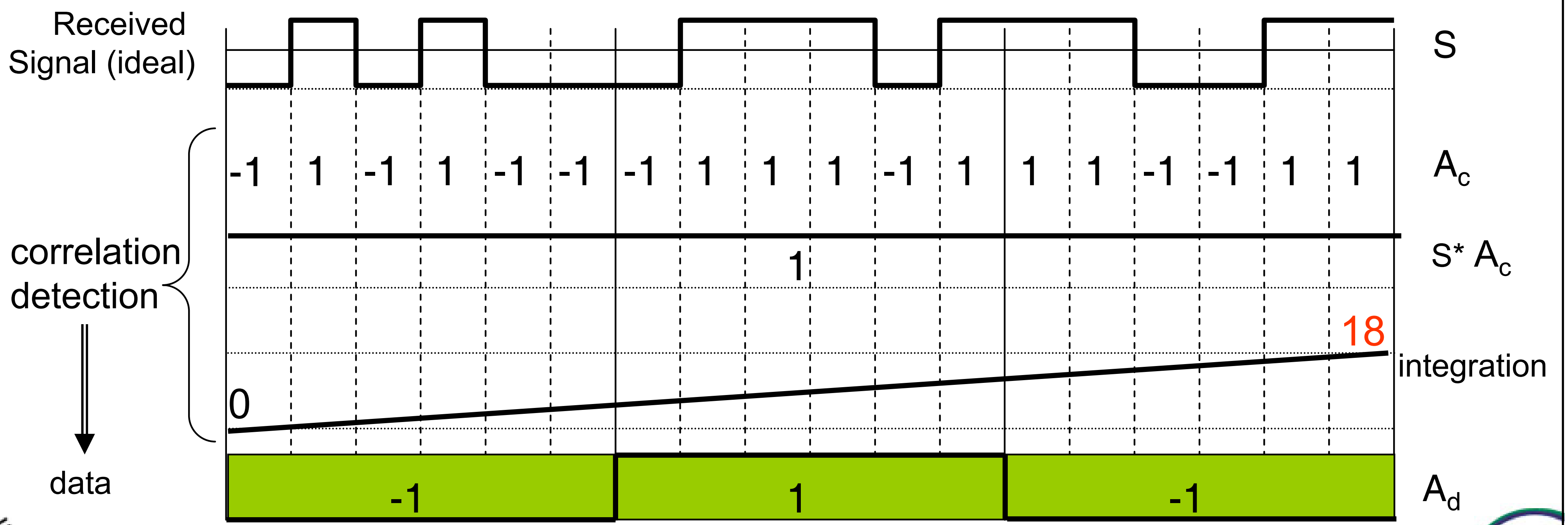
modulation scheme

DSSS in time domain

Transmitter: spreading

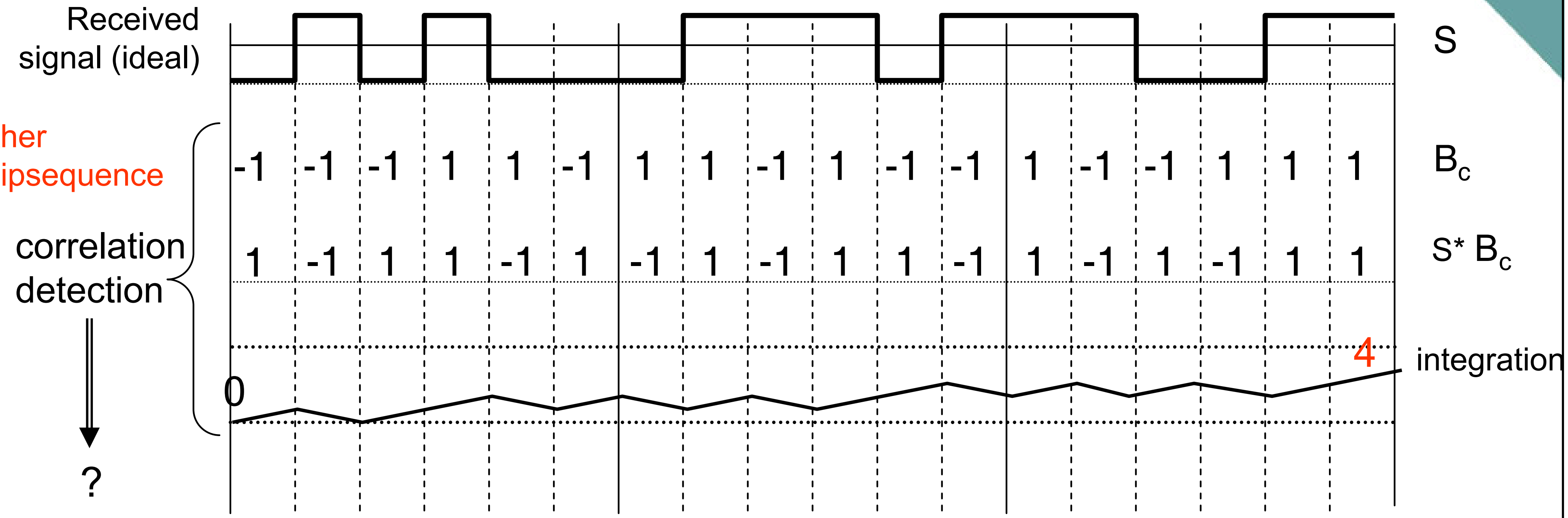


Receiver: despreading



DSSS in time domain

Receiver:



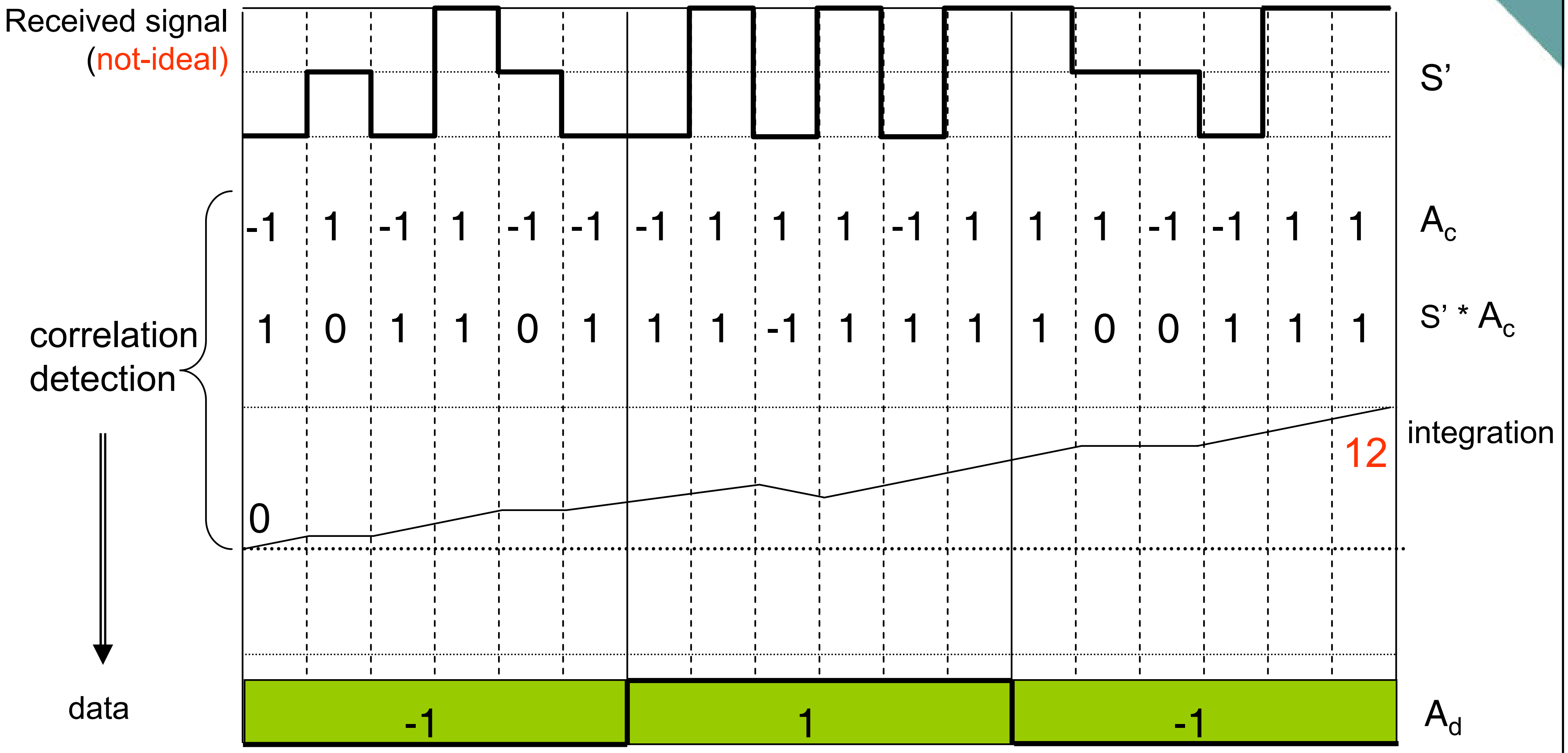
B_c	-1	-1	-1	1	1	-1	1	1	-1	1	-1	-1	1	-1	-1	1	1	1
$S^* B_c$	1	-1	1	1	-1	1	-1	1	-1	1	1	-1	1	-1	1	-1	1	1

With orthogonal sequences: result correlation = 0
In quasi-orthogonale codes: result correlation = ‘small’

cfr. WiFi : Barker codes

DSSS in time domain

Receiver:



Received signal (not-ideal)

S'

correlation detection

A_c	-1	1	-1	1	-1	-1	-1	1	1	1	-1	1	1	1	-1	-1	1	1
$S' * A_c$	1	0	1	1	0	1	1	1	-1	1	1	1	1	0	0	1	1	1

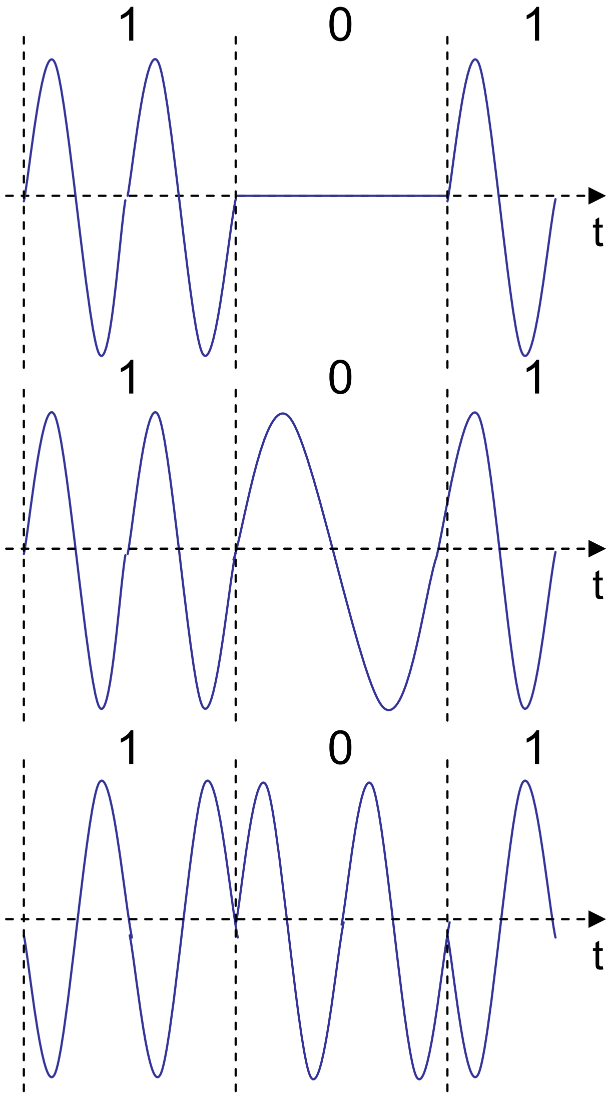
integration

data

A_d	-1	1	-1

Modulation schemes

- Modulation of digital signals -> Shift Keying
- Amplitude Shift Keying (ASK):
  - simple
  - Small bandwidth required
  - Very sensitive for interference
- Frequency Shift Keying (FSK):
- Phase Shift Keying (PSK):
  - Large bandwidth required
  - robust against interference
  - More complex



MSK

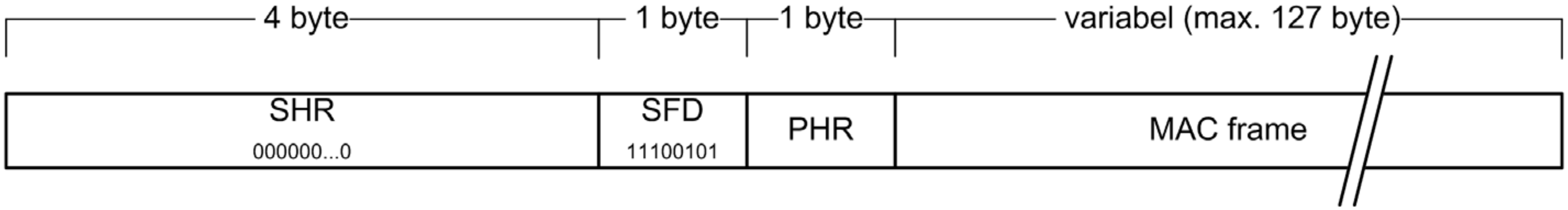
- FSK without phase jumps: continuous phase FSK (CFSK)
- Bandwidth necessary for FSK depends on the distance between the used current frequencies

- MSK : Minimum Shift-Keying
  - Minimum distance between the used frequencies and still orthogonal
  - CFSK via carefully defined phase variations

- In IEEE802.15.4:

  O-QPSK with sinusoidal pulse shape = MSK

Physical frame



SHR : synchronisation header (32 zeros)
SFD : start frame delimiter
PHR : physical frame header : 7 LSB indicate the length of the MAC frame

Functional discription

- Physical layer responsible for
  - Data transmission
  - Activation and deactivation of the radio

    Transmitting, receiving or sleeping, decided by upper layer
  - Received energy detection (ED)

    Energy detection in the channel (for 8Ts), no decoding
  - Link Quality Indication (LQI)

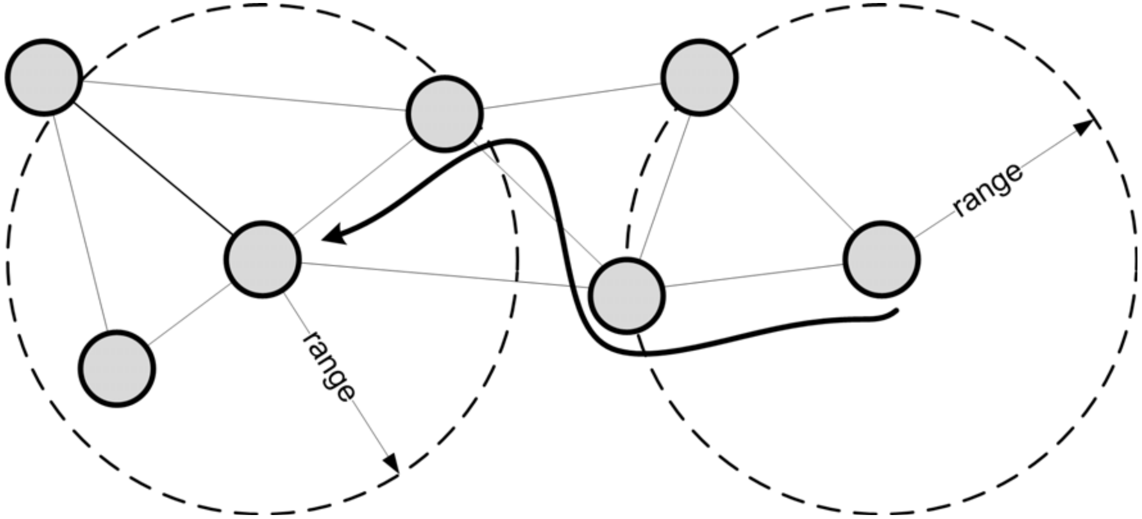
    via ED and/or estimation of the SNR
  - Clear Channel Assessment

    Report of the state of the medium, *busy* or *idle* (Important for MAC!)
    - Energy Detection mode
    - Carrier Sense mode
    - Carrier Sense with Energy Detection mode
  - Channel selection
  - Transmission power

Range

- Range : strongly dependents on environment
  - Outdoor, open space: > 1km
  - Outdoor, urban: <200m
  - Indoor, good circumstances: <100m
  - Indoor, practical: 30-50m

- Transmit power
  - Between 0.5 and 100 mW

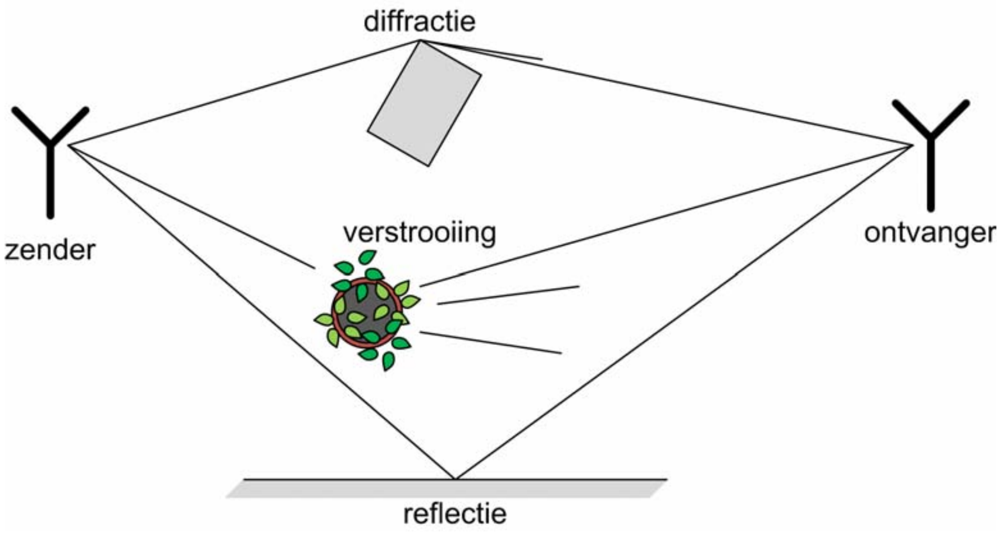


Indoor radio propagation

- In free space: signal travels via a straight line (LOS),
  Received power decreases with the distance d between the transmitter and the receiver

$$P \sim \frac{1}{d^2}$$

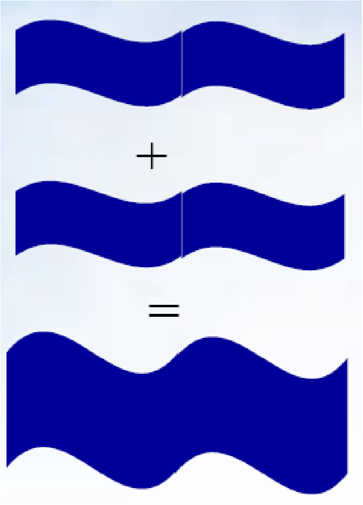
- Indoor : multi path propagation caused by
  - reflection
  - scattering
  - diffraction



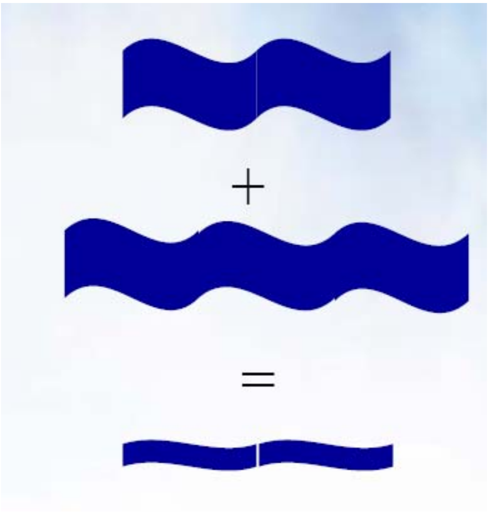
Signal Strength

Multipath propagation

Two signals with a difference in path length of λ



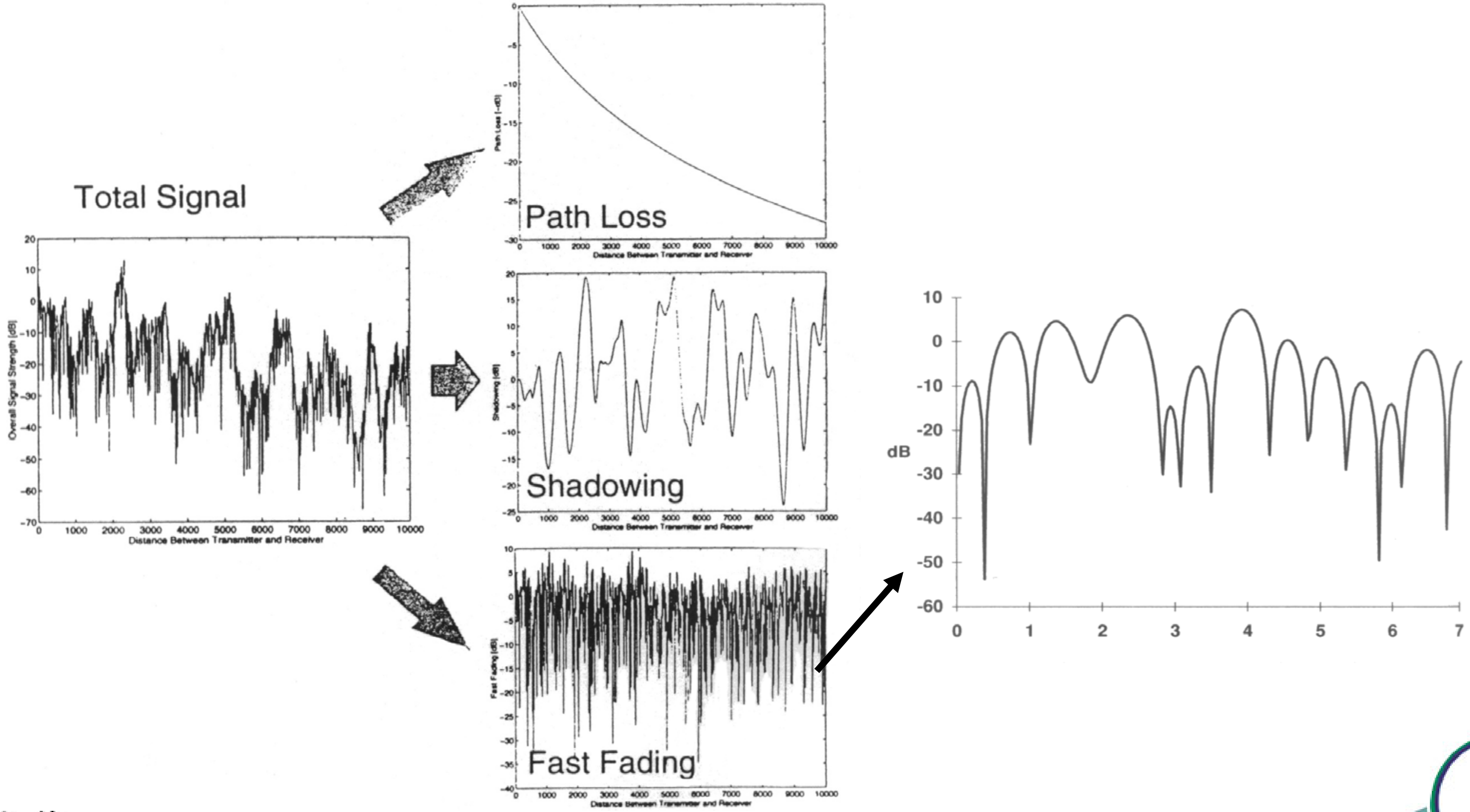
Two signals with a difference in path length of λ/2



Frequency dependent

Signal Strength

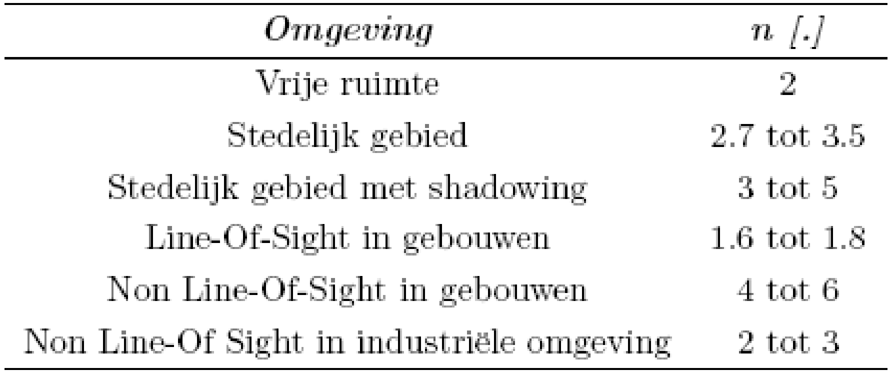
- **Multipath propagation:** phase relation between the signals depends on position and frequency => strong variations in signal strength (constructive en destructive interference)



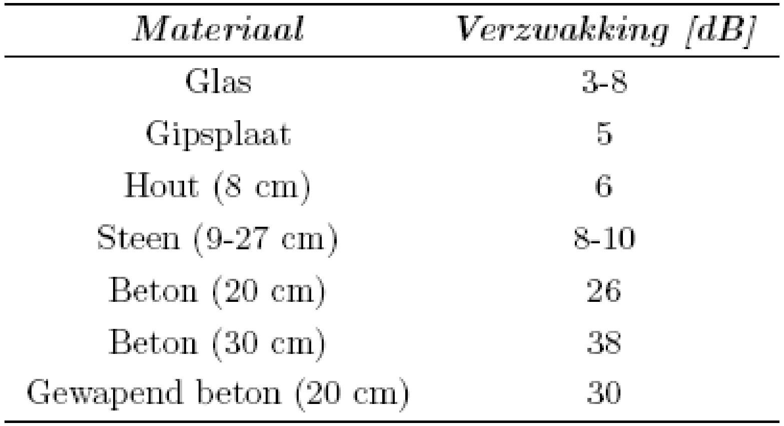
Signal Strength

- Received power decreases faster with the distance

$$P \sim \frac{1}{d^n}$$

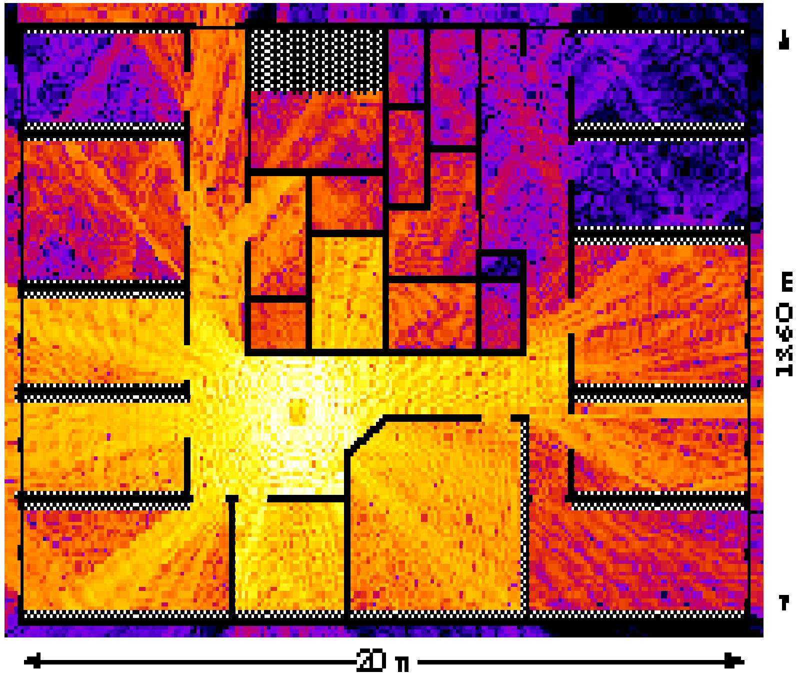


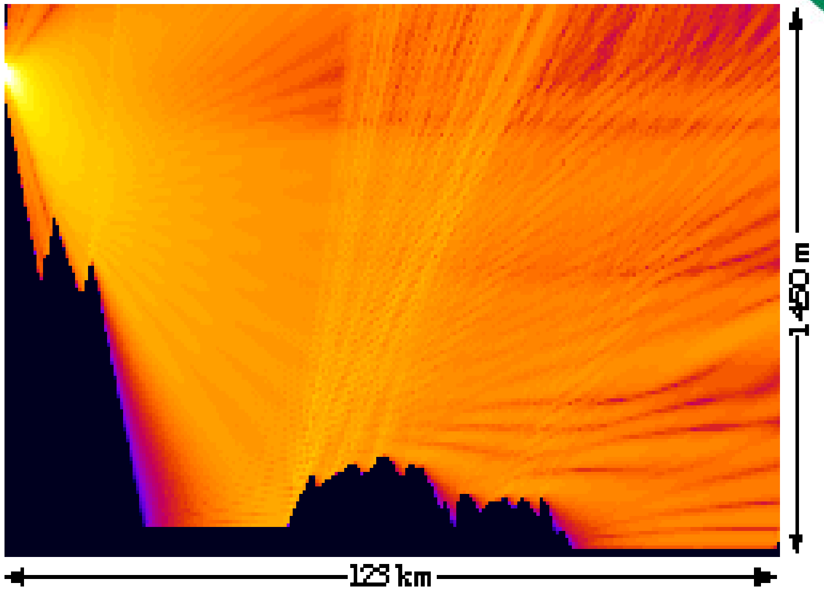
Omgeving	*n [.]*
Vrije ruimte	2
Stedelijk gebied	2.7 tot 3.5
Stedelijk gebied met shadowing	3 tot 5
Line-Of-Sight in gebouwen	1.6 tot 1.8
Non Line-Of-Sight in gebouwen	4 tot 6
Non Line-Of Sight in industriële omgeving	2 tot 3

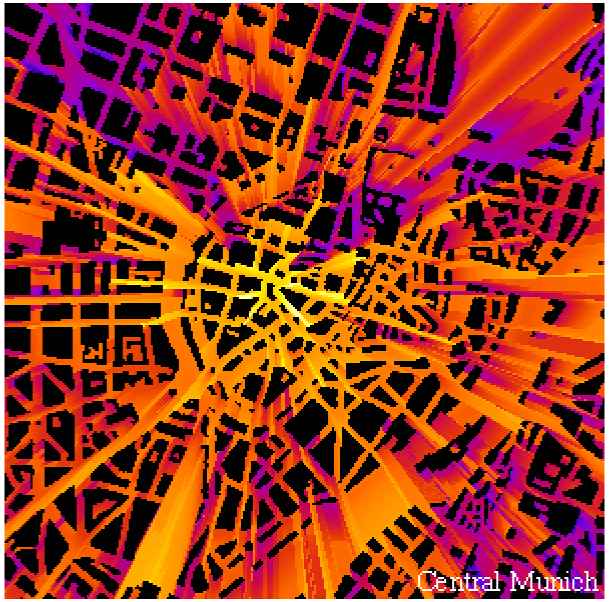


Materiaal	*Verzwakking [dB]*
Glas	3-8
Gipsplaat	5
Hout (8 cm)	6
Steen (9-27 cm)	8-10
Beton (20 cm)	26
Beton (30 cm)	38
Gewapend beton (20 cm)	30

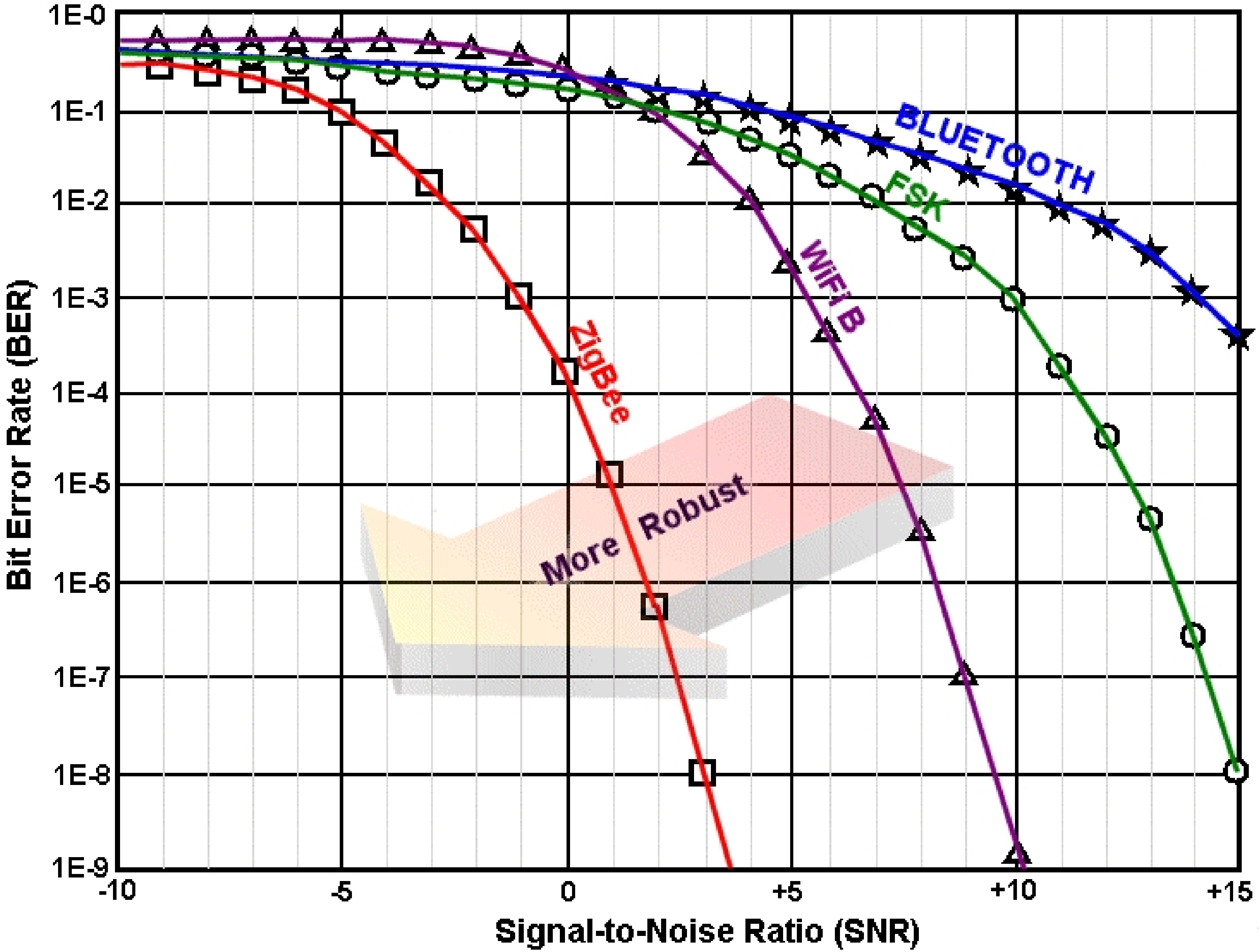
Signal Strength







Physical Layer



ZigBee – Medium Access Control Layer (MAC)

Anneleen Van Nieuwenhuyse

KaHo Sint-Lieven – DraMCo – 21/05/2009

Overview

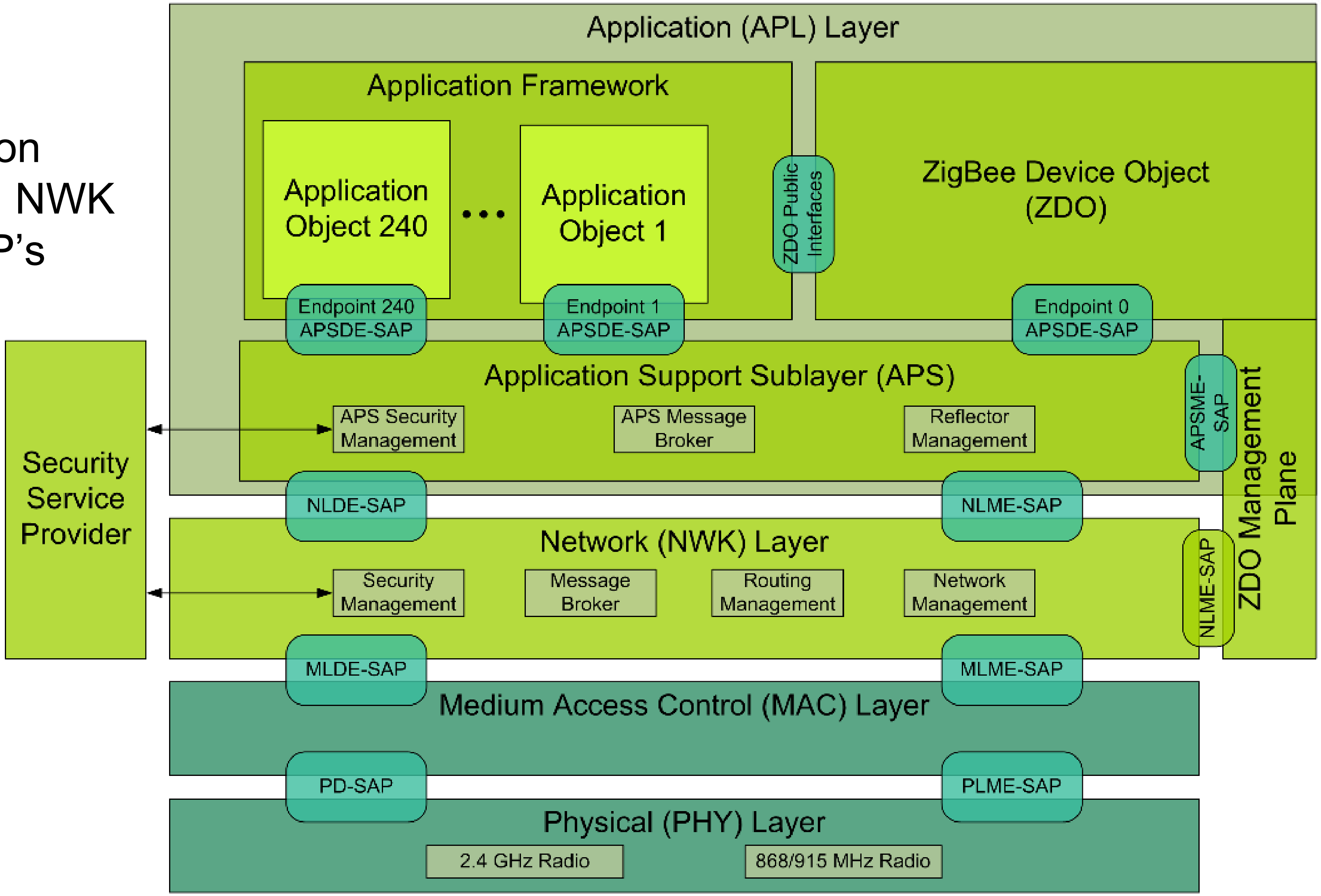
- Introduction
- Addresses
- Frame structure
- Operational modes
- Data transfer model
- MAC Services

MAC Layer: General

- Realise a reliable connection (MAC) on top of an unreliable medium (PHY)
  - Addresses
  - Fault control
  - Receive acknowledgment
  - Control the channel access
- Provide services to the upper layer (NWK)
  - Make connections between devices (association)
  - Data transmission

ZigBee Protocol stack

Communication with PHY and NWK Layer via SAP's



🟩 IEEE 802.15.4

🟩 ZigBee^{TM} Alliance

🟩 End manufacturer

🟩 Layer Function

🟩 Layer Interface

Addresses

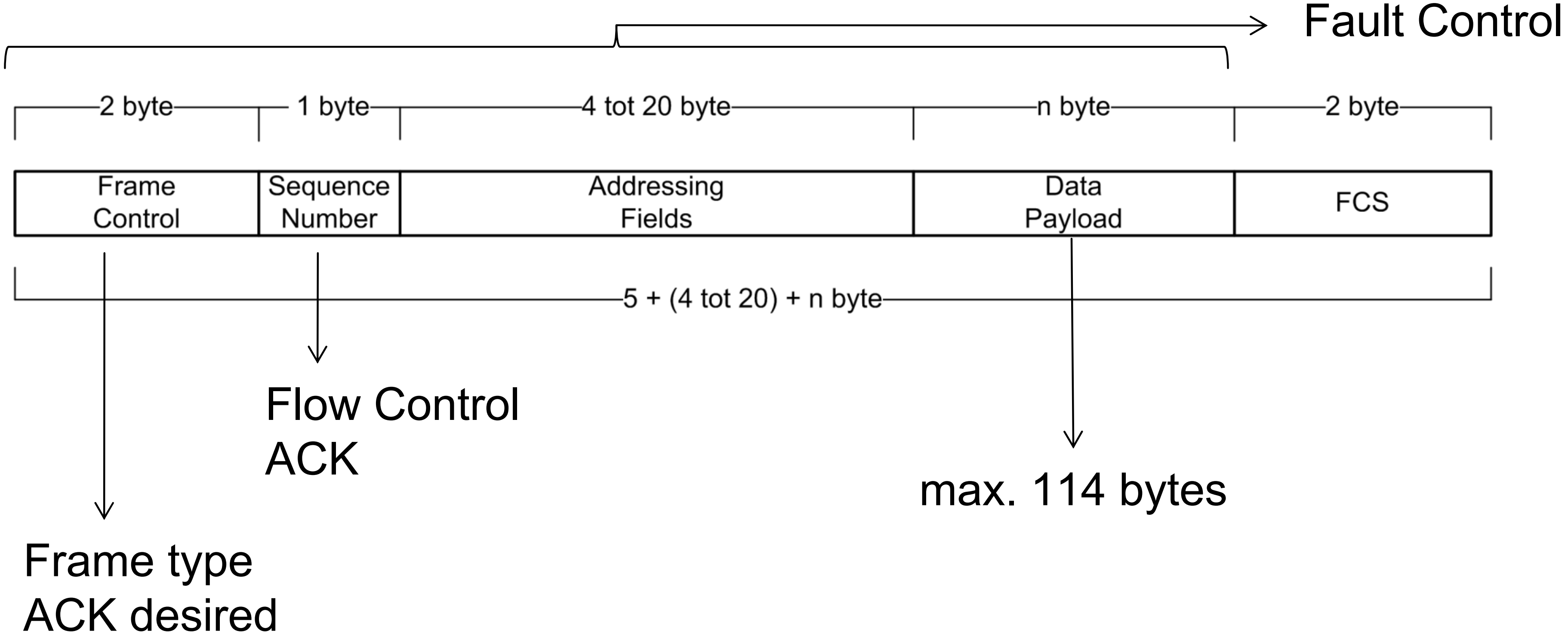
- 64 bit IEEE extended address (MAC address)
  - Unique
- 16 bit short address
  - Unique inside the network
  - 65535 nodes (+ co-ordinator) in 1 PAN → scalability
- Each network has an unique PAN ID (16 bit)

General frame structure

- MAC frame = PHY payload
- 4 types
  - Data
  - Acknowledgement
  - MAC command
  - Beacon
- Common part
  - Frame control
  - Sequence number
  - Addressing fields (except ACK)
  - Frame Check Sequence (16 bit CRC)

Data frame

Goal: Transmit application data from higher layers



Fault Control

2 byte	1 byte	4 tot 20 byte	n byte	2 byte
Frame Control	Sequence Number	Addressing Fields	Data Payload	FCS

5 + (4 tot 20) + n byte

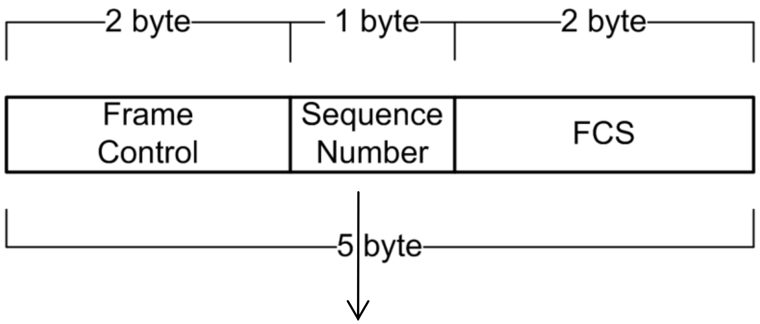
Frame type
ACK desired

Flow Control
ACK

max. 114 bytes

ACK frame

Goal: Confirmation of received frames



2 byte	1 byte	2 byte
Frame Control	Sequence Number	FCS

5 byte

Equal to the sequence number of the frame that needs confirmation

Command frame

Goal: Give assignments or requests

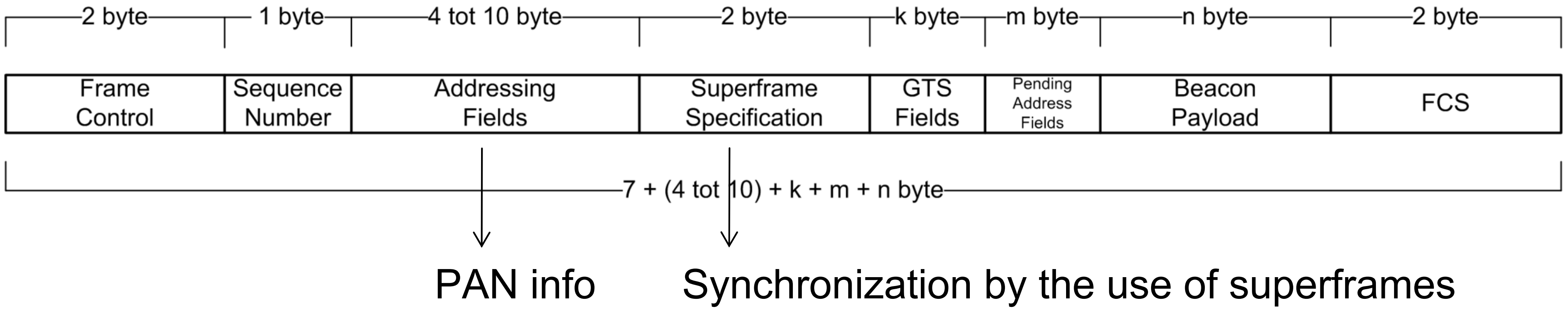
- association request
- data request

Frame Control	Sequence Number	Addressing Fields	Command Type	Command Payload	FCS
2 byte	1 byte	4 tot 20 byte	1 byte	n byte	2 byte

6 + (4 tot 20) + n byte

Beacon frame

Goal: Pass information concerning the PAN synchronization in the network



2 byte	1 byte	4 tot 10 byte	2 byte	k byte	m byte	n byte	2 byte
Frame Control	Sequence Number	Addressing Fields	Superframe Specification	GTS Fields	Pending Address Fields	Beacon Payload	FCS

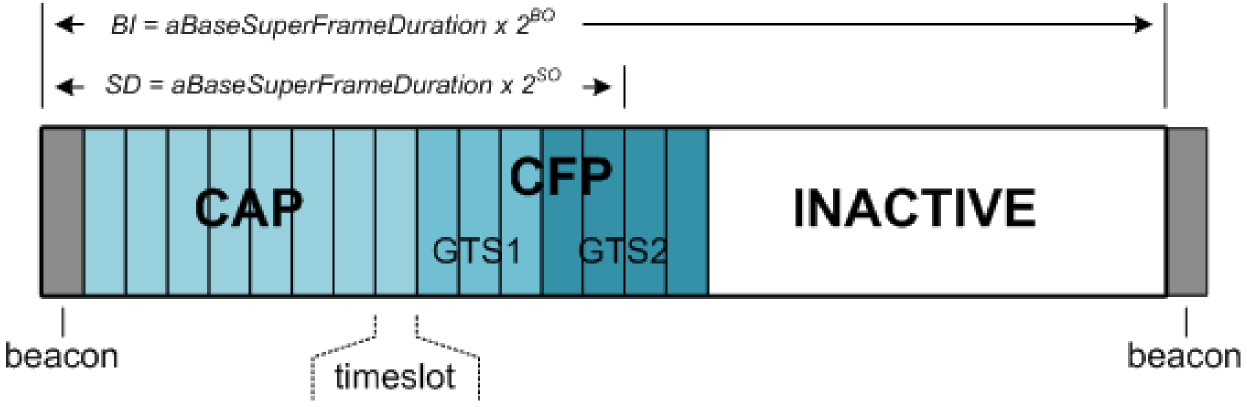
7 + (4 tot 10) + k + m + n byte

PAN info

Synchronization by the use of superframes

Operational modes

- Beacon-enabled
  - Superframes
  - Slotted CSMA/CA

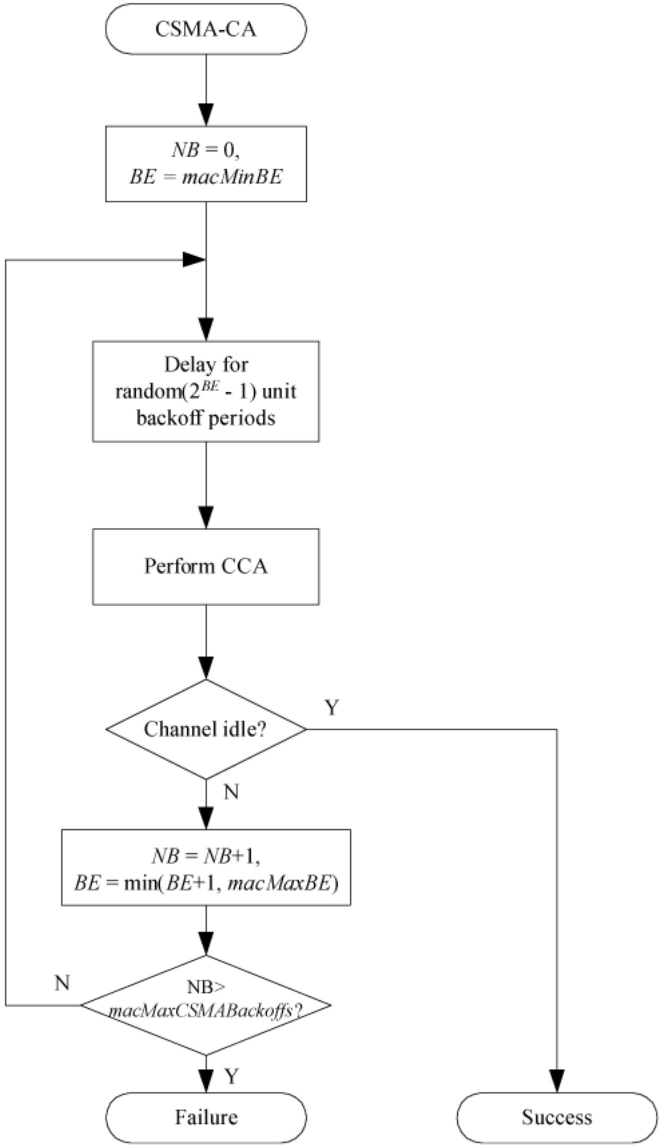

BI = aBaseSuperFrameDuration x 2^BO
SD = aBaseSuperFrameDuration x 2^SO
CAP
CFP
GTS1
GTS2
INACTIVE
beacon
timeslot
beacon

$0 \leq BO \leq 14$
$0 \leq SO \leq BO \leq 14$

- Nonbeacon-enabled
  - Used by ZigBee
  - Unslotted CSMA/CA
  - Beacons used for transmission of network information

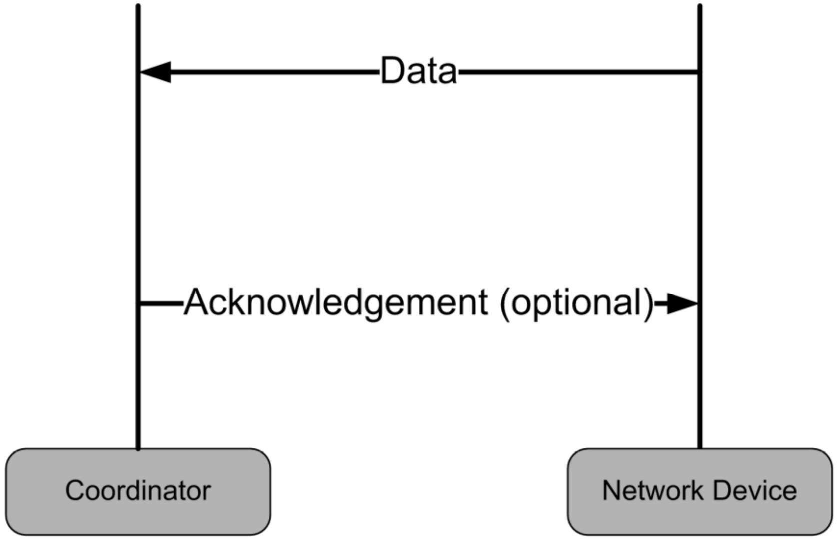
CSMA/CA

- CS: Carrier Sense
  - CCA (listening)
- MA: Multiple Access
  - Shared medium
- CA: Collision Avoidance
  - Random backoff

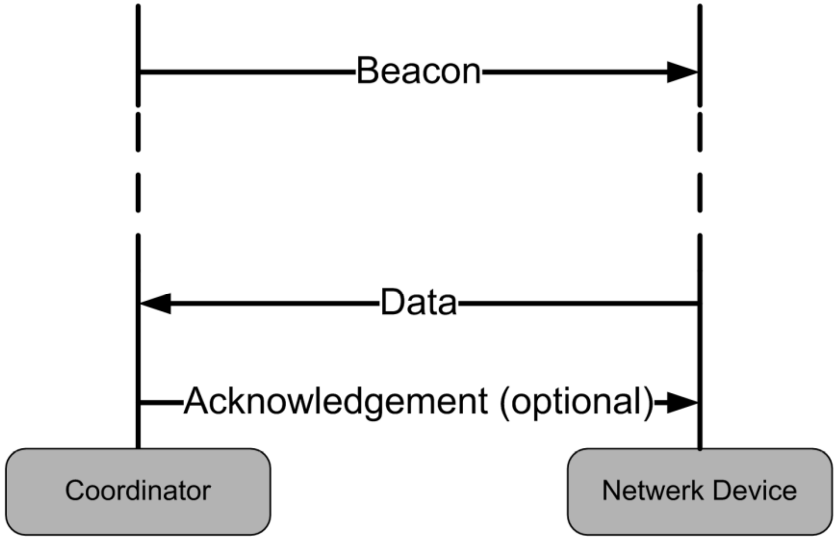


Data transfer model: Towards the co-ordinator

The coordinator is always active → Sending data is always possible



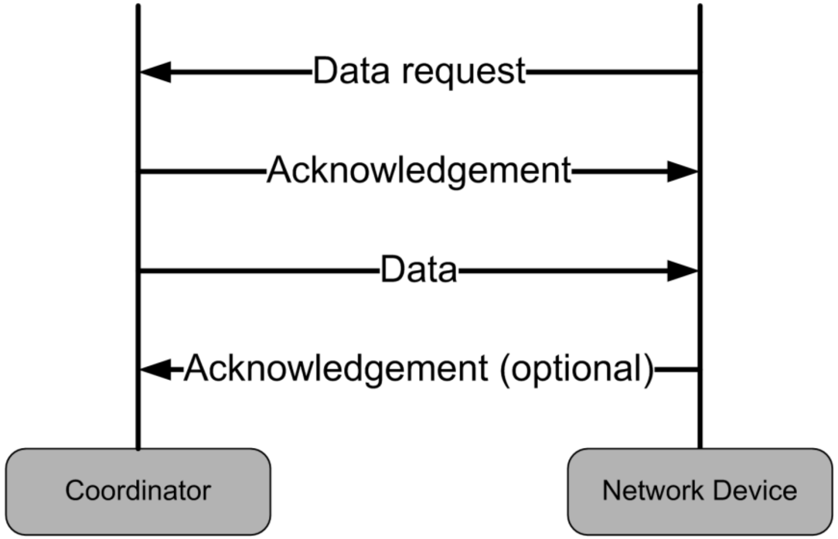
nonbeacon-enabled



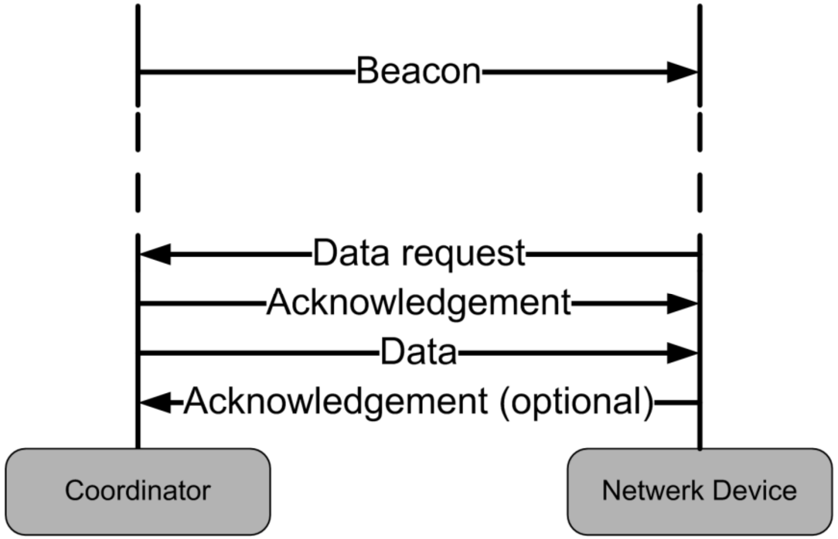
beacon-enabled

Data transfer model: From the co-ordinator

The RFD’s aren’t always active
→ they ask themselves if data is available



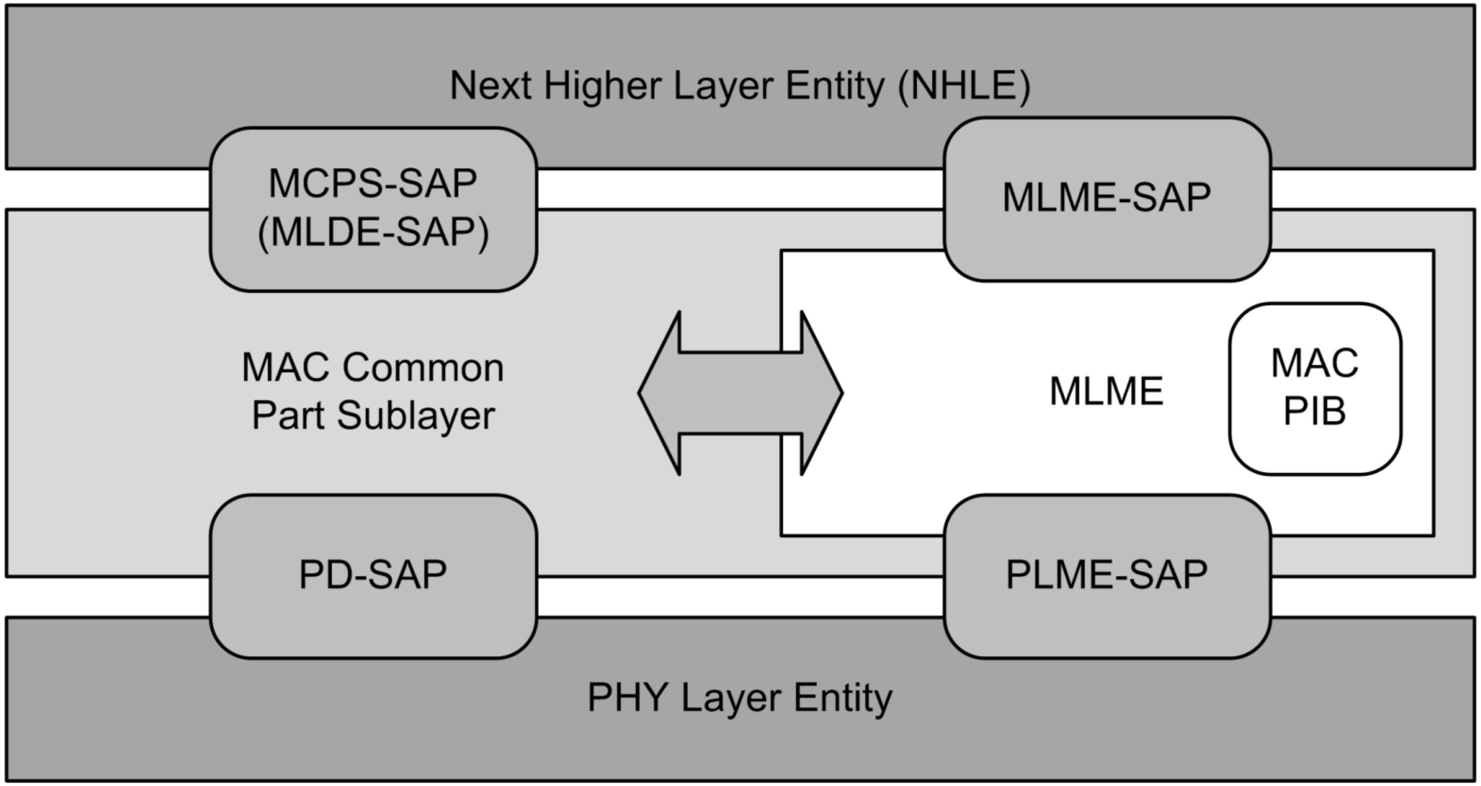
nonbeacon-enabled



beacon-enabled

MAC Services in general

- Service Access Points (SAP's)
- Management Entity (MLME)
- Data Entity (MCPS / MLDE)



Data Service

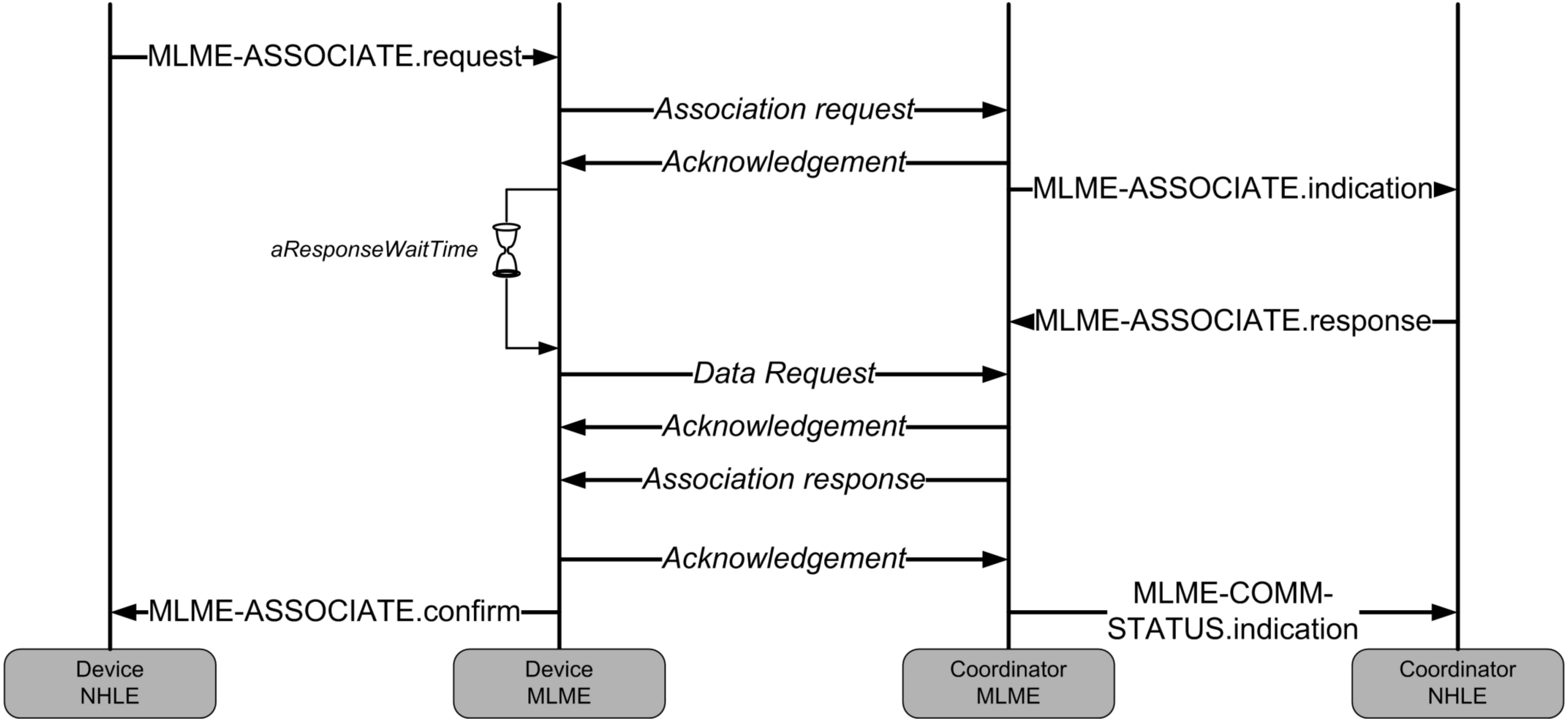
- MLDE-DATA
  - Request (ask for transmission)
  - Confirm (confirmation of the transmission)
  - Indication (reception of data)
- MLDE-PURGE
  - Delete messages in the queue

Management Service

- MLME-GET
  - Retrieve information from the MAC IB
- MLME-SET
  - Change information in the MAC IB
- MLME-SCAN
  - ‘measure’ the activities in a specific channel
  - Start-up of a PAN
  - Join a PAN

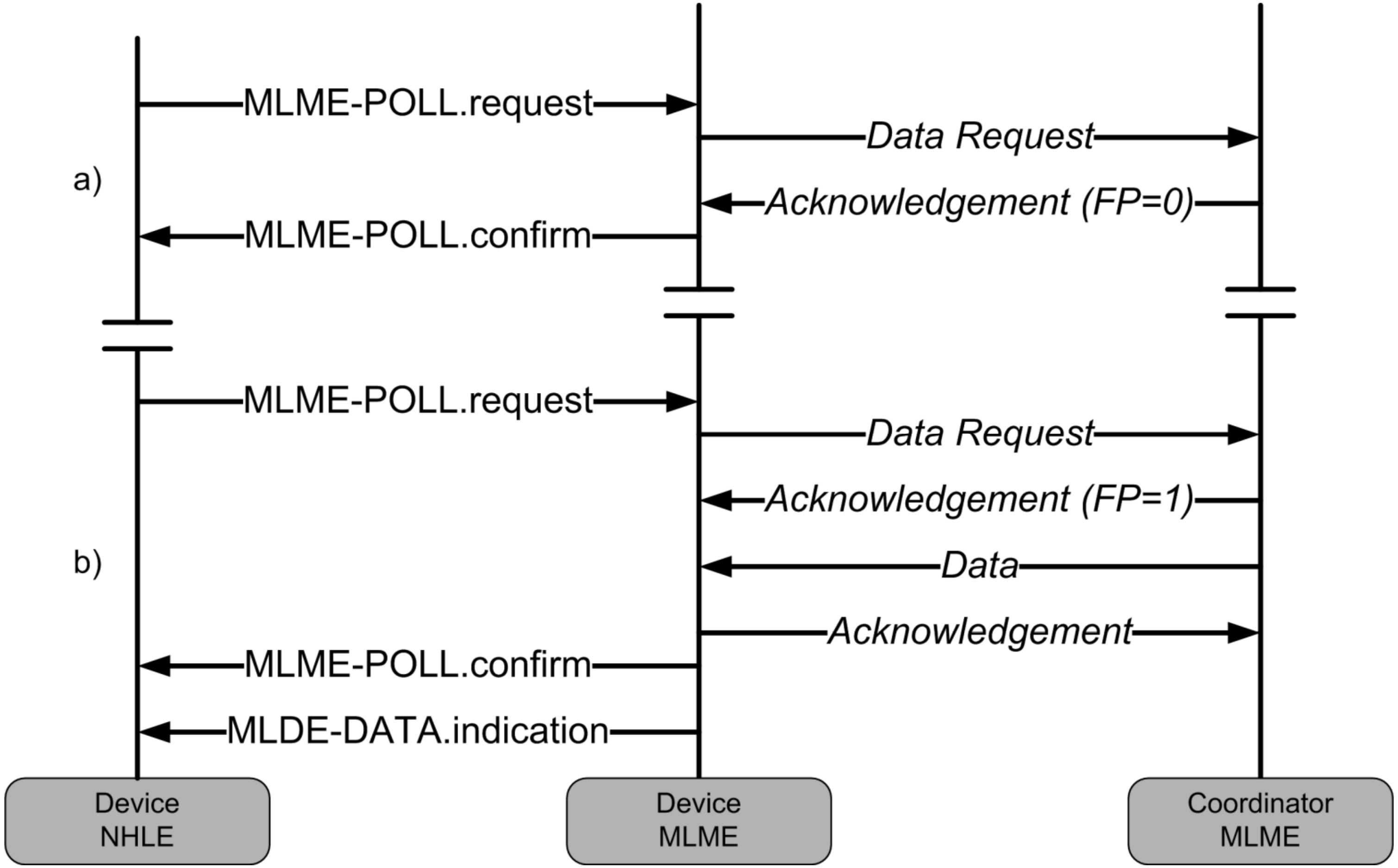
Management Service

- MLME-ASSOCIATE



Management Service

- MLME-POLL



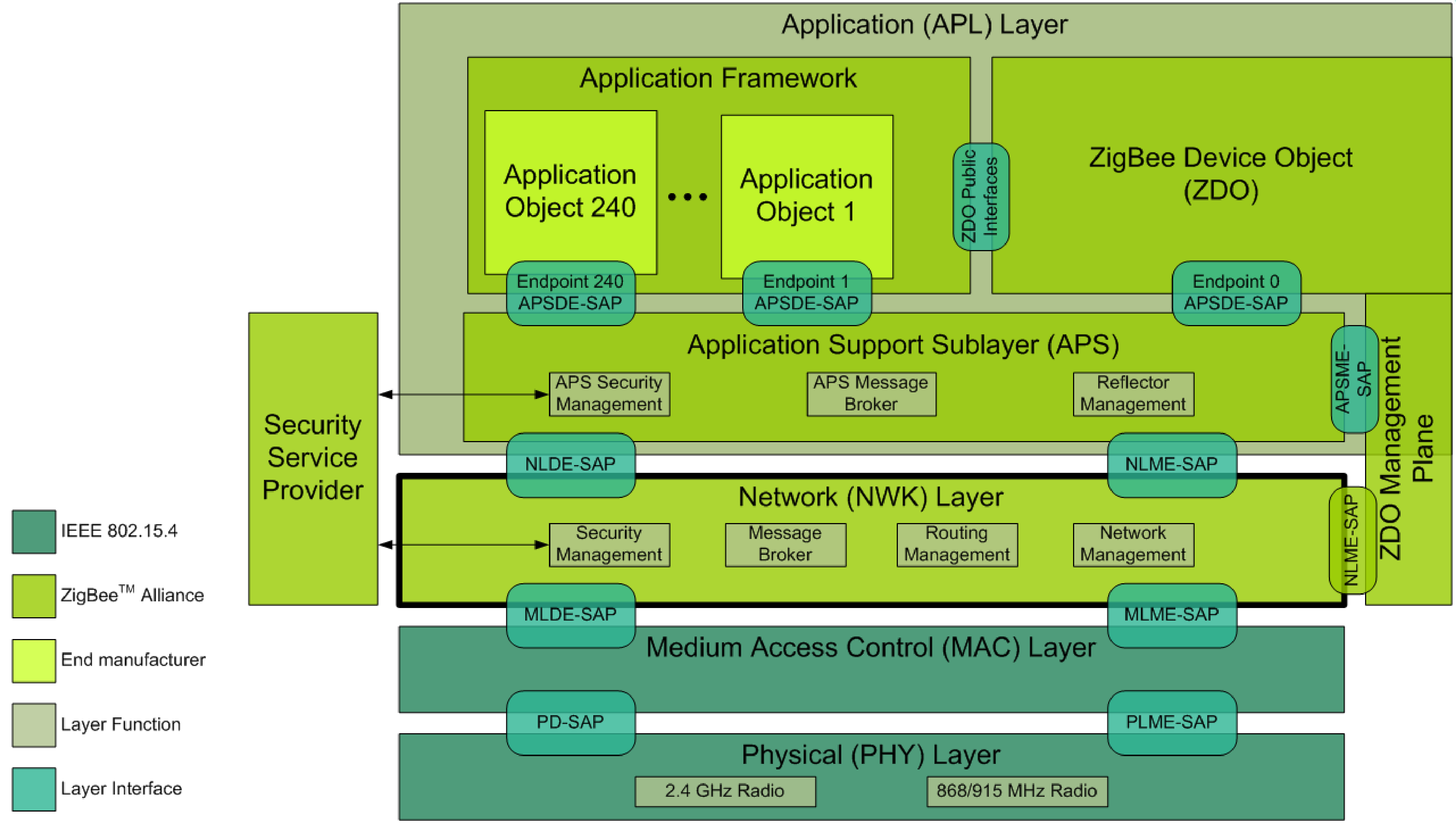
ZigBee – Network Layer

Anneleen Van Nieuwenhuyse
KaHo Sint-Lieven – DraMCo – 21/05/2009

Overview

- Introduction
- Overview of the Network Layer
  - Data Service Access Point
  - Management Service Access Point
- Maintenance of the network and the devices
  - Start-up of a new network
  - Temporarily provide access to the network for devices
  - Network Discovery
  - Join the network
  - Leave the network
  - Neighbour tables
  - Address assignment
- Routing

Introduction

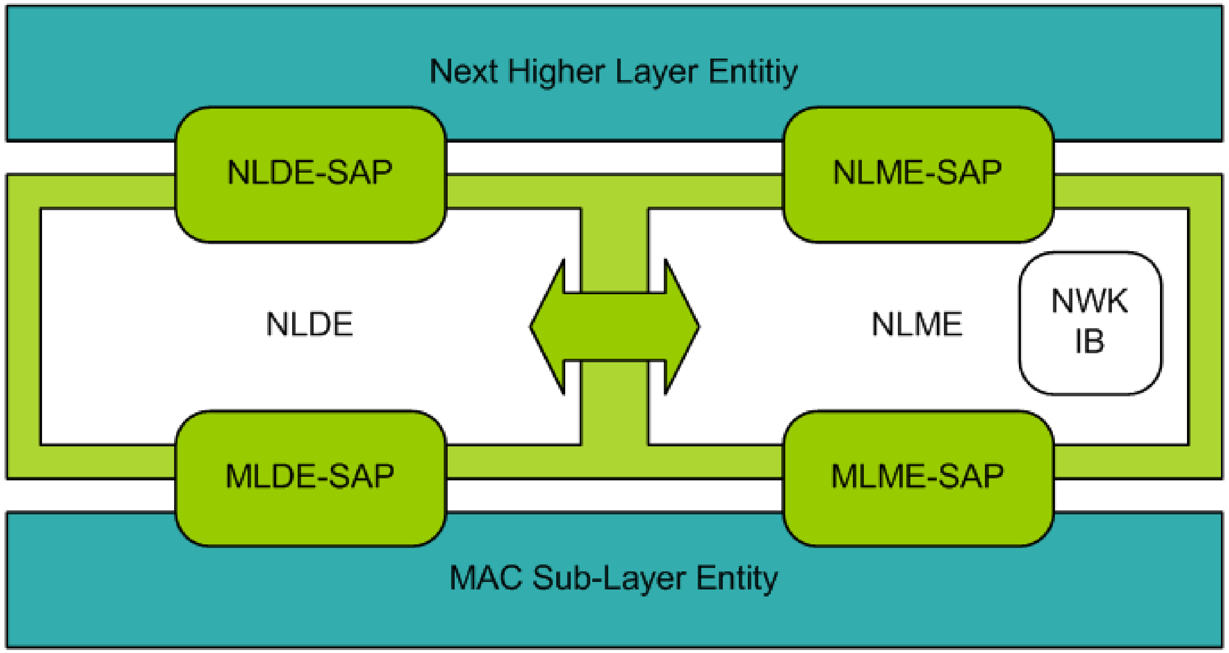


Introduction

- Main functionalities:
  - Building a network by a ZigBee Co-ordinator
  - Allow devices temporarily to join the network
  - Build the network topology
  - Distribute network addresses
  - Routing of data packets through the network
  - Security

Overview of the Network Layer

- 2 important service entities
  - Data Service Entity
  - Management Service Entity



Overview of the Network Layer

- Network Layer Data Entity (NLDE):
  - Generation of data packets (NPDU) by adding a header to data (APDU) coming from the APS sub-layer
  - Topology specific routing
  - Security: Ensure authentication and confidentiality of messages

NLDE-SAP Primitive	*Request*	*Confirm*	*Indication*
NLDE-DATA	x	x	x

Overview of the Network Layer

- Network Layer Management Entity (NLME):
  - Initialisation of the nodes (ZED, ZR, ZC)
  - Start-up of the network
  - Allow nodes to enter the network
  - Distribution of the network addresses
  - Search for neighbour devices
  - Establish routes throughout the network
  - Routing to unicast-, multicast- en broadcast addresses

Overview of the Network Layer

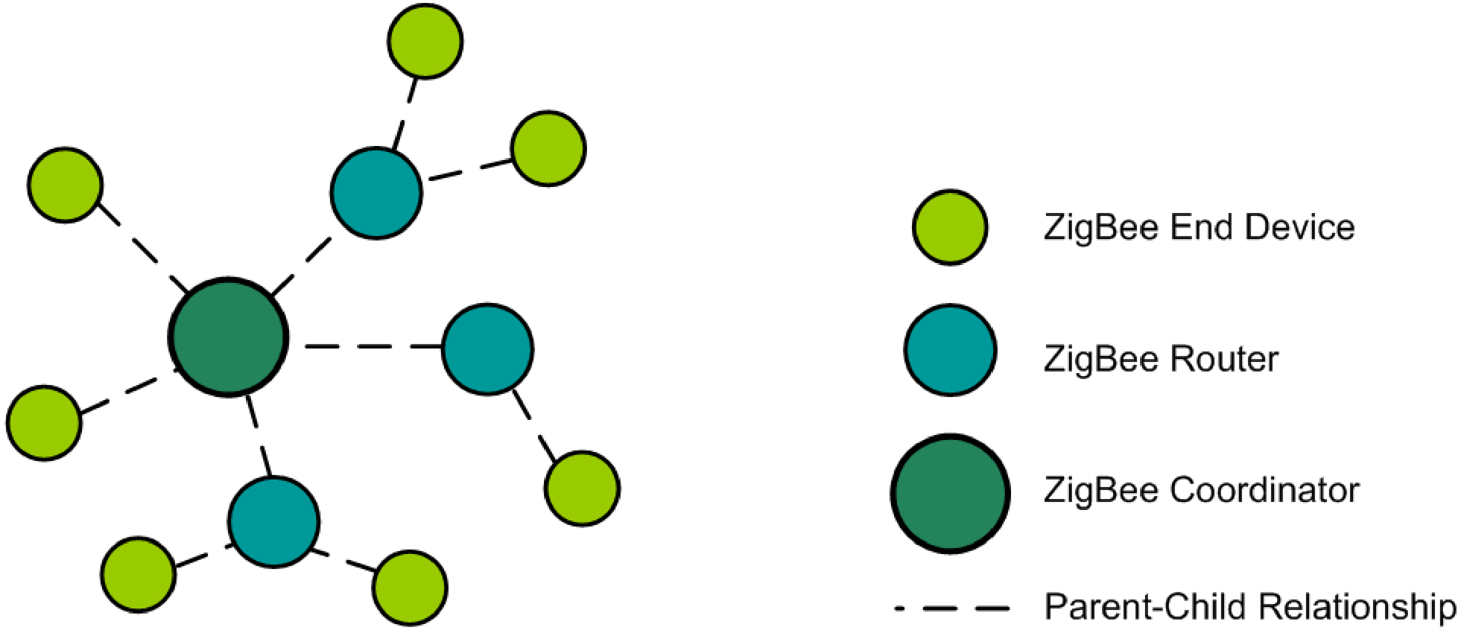
- Network Layer Management Entity (NLME):

NLME-SAP Primitive	*Request*	*Confirm*	*Indication*
NLME-NETWORK DISCOVERY	x	x	
NLME-NETWORK-FORMATION	x	x	
NLME-PERMIT-JOINING	x	x	
NLME-START-ROUTER	x	x	
NLME-ED-SCAN	x	x	
NLME-JOIN	x	x	x
NLME-DIRECT-JOIN	x	x	
NLME-LEAVE	x	x	x
NLME-RESET	x	x	
NLME-SYNC	x	x	
NLME-SYNC-LOSS			x
NLME-GET	x	x	
NLME-SET	x	x	
NLME-NWK-STATUS			x
NLME-ROUTE-DISCOVERY	x	x	

Maintenance of the network and the devices

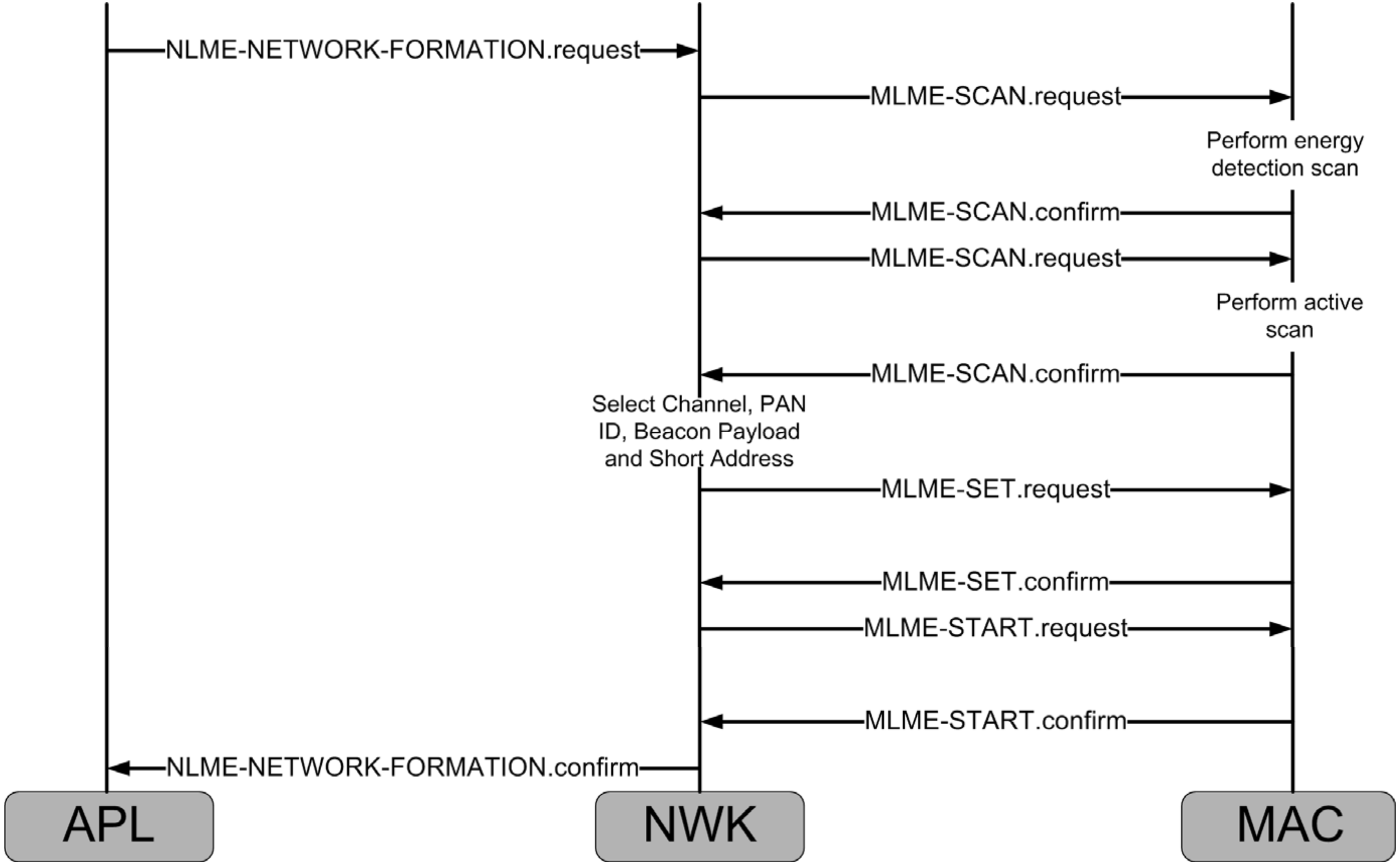
- Start-up of a new network
- Allow devices temporarily to join the network
- Network Discovery

- Join a network
- Leave the network
- Neighbour tables
- Address distribution



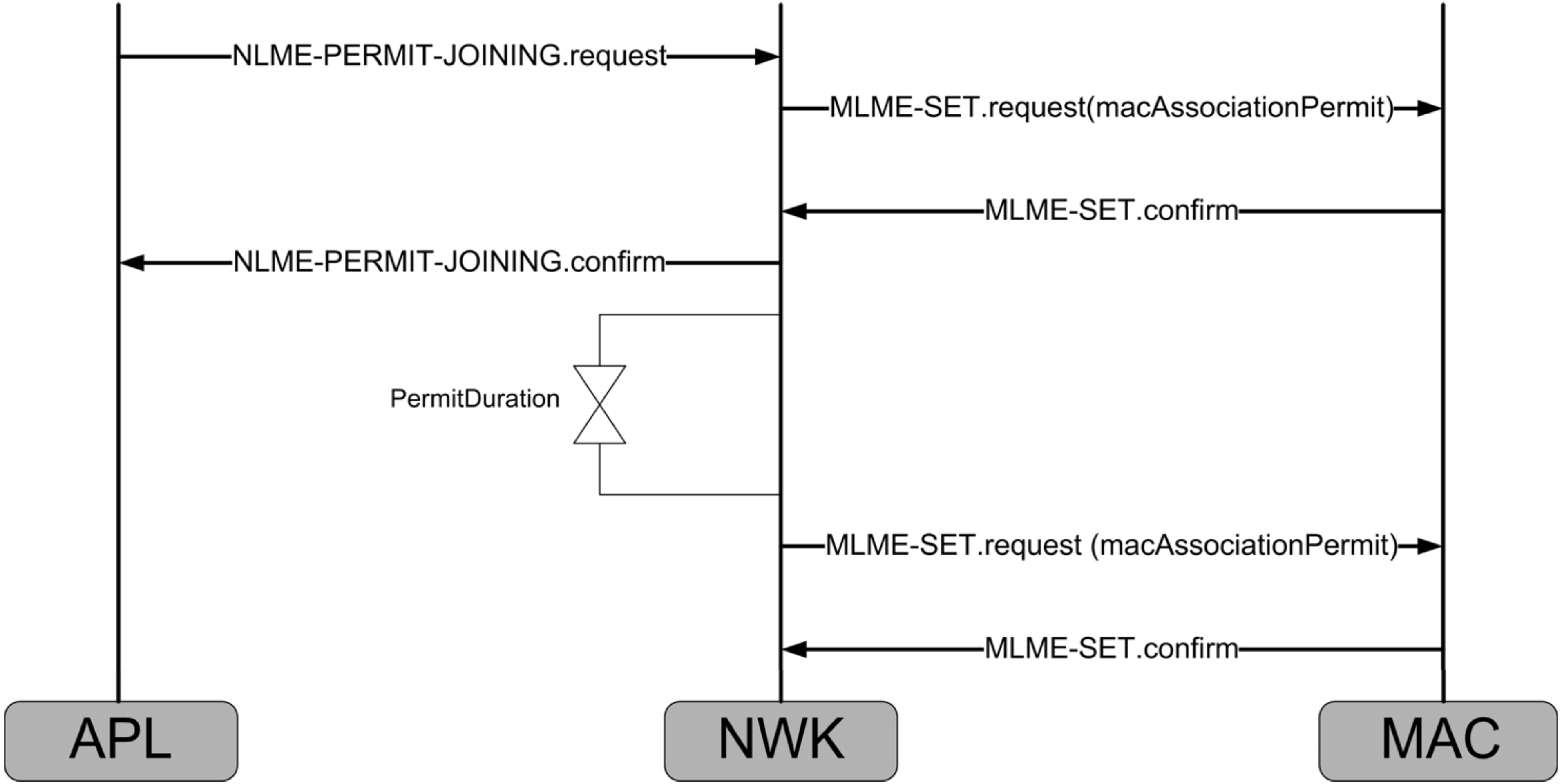
Maintenance of the network and the devices

- Start-up of a network (ZC)



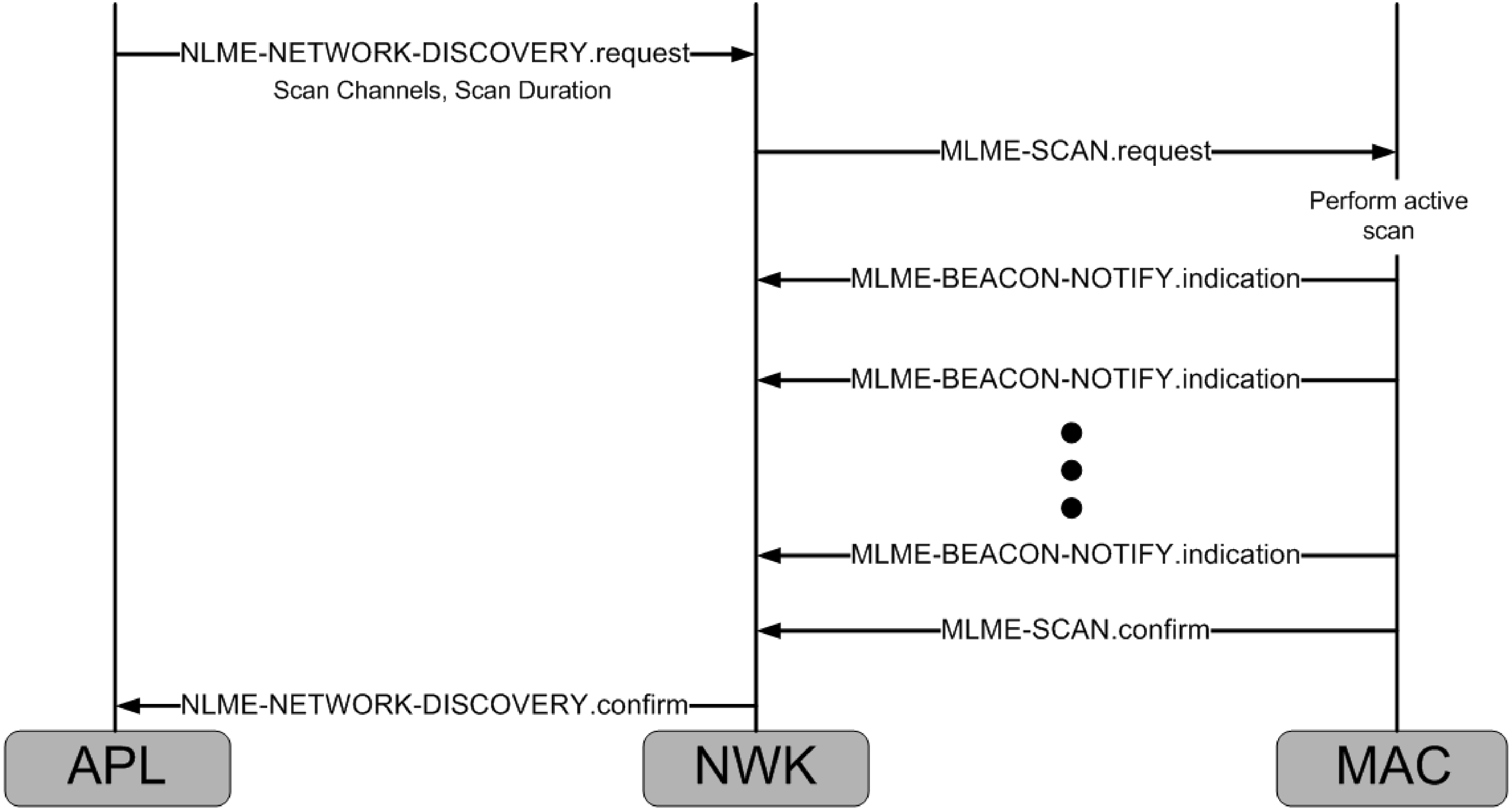
Maintenance of the network and the devices

- Temporarily allow devices to join the network (ZR en/of ZC)


NLME-PERMIT-JOINING.request
MLME-SET.request(macAssociationPermit)
MLME-SET.confirm
NLME-PERMIT-JOINING.confirm
PermitDuration
MLME-SET.request (macAssociationPermit)
MLME-SET.confirm
APL
NWK
MAC

Maintenance of the network and the devices

- Network Discovery: Which networks are available in the neighbourhood of the device


NLME-NETWORK-DISCOVERY.request
Scan Channels, Scan Duration
MLME-SCAN.request
Perform active scan
MLME-BEACON-NOTIFY.indication
MLME-BEACON-NOTIFY.indication
MLME-BEACON-NOTIFY.indication
MLME-SCAN.confirm
NLME-NETWORK-DISCOVERY.confirm
APL
NWK
MAC

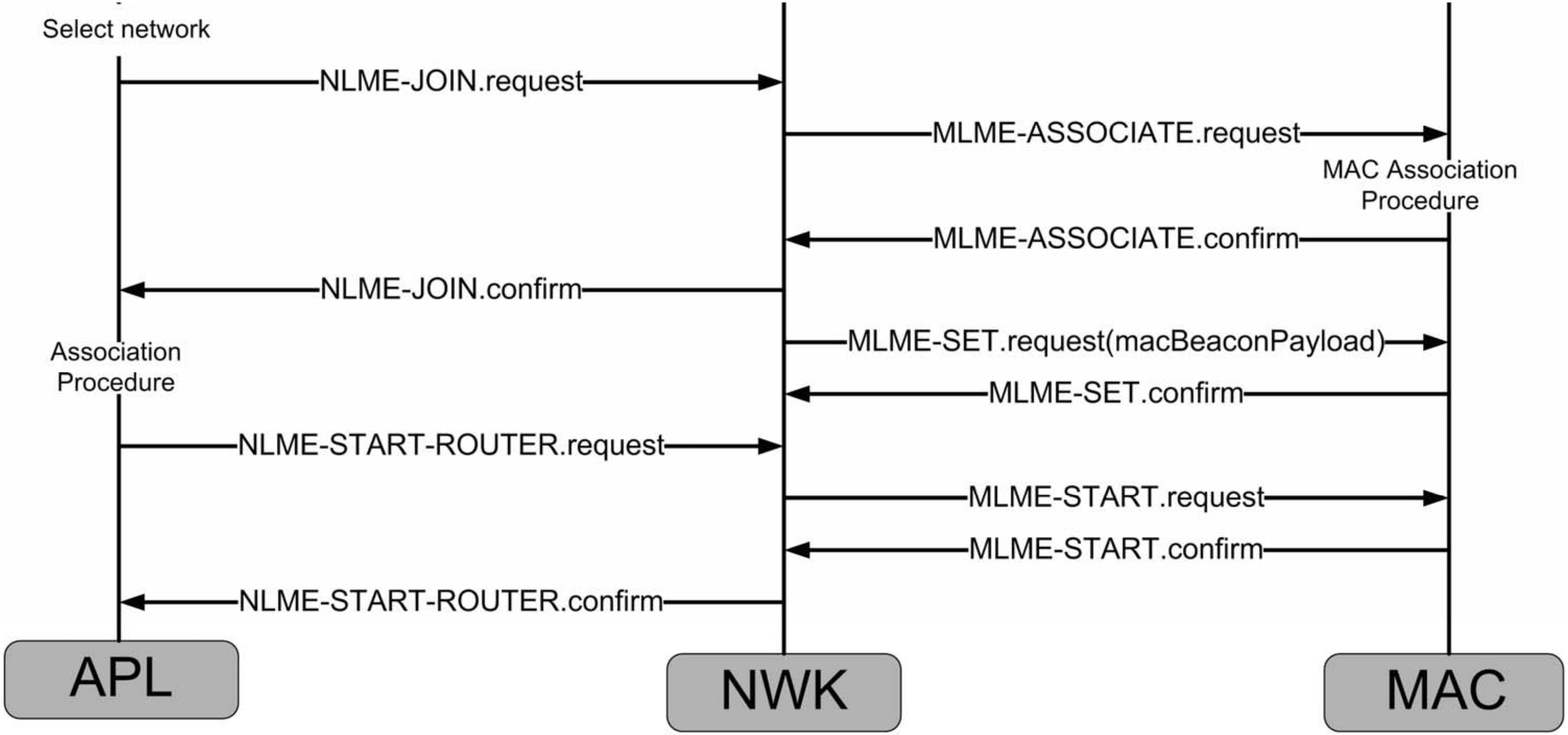
Maintenance of the network and the devices

- Join the network
  - Join through association
  - Join or rejoin through NWK Rejoin
  - Join directly
  - Join or rejoin through orphaning

- Procedures should be observed from two sides:
  - Child procedure
  - Parent procedure

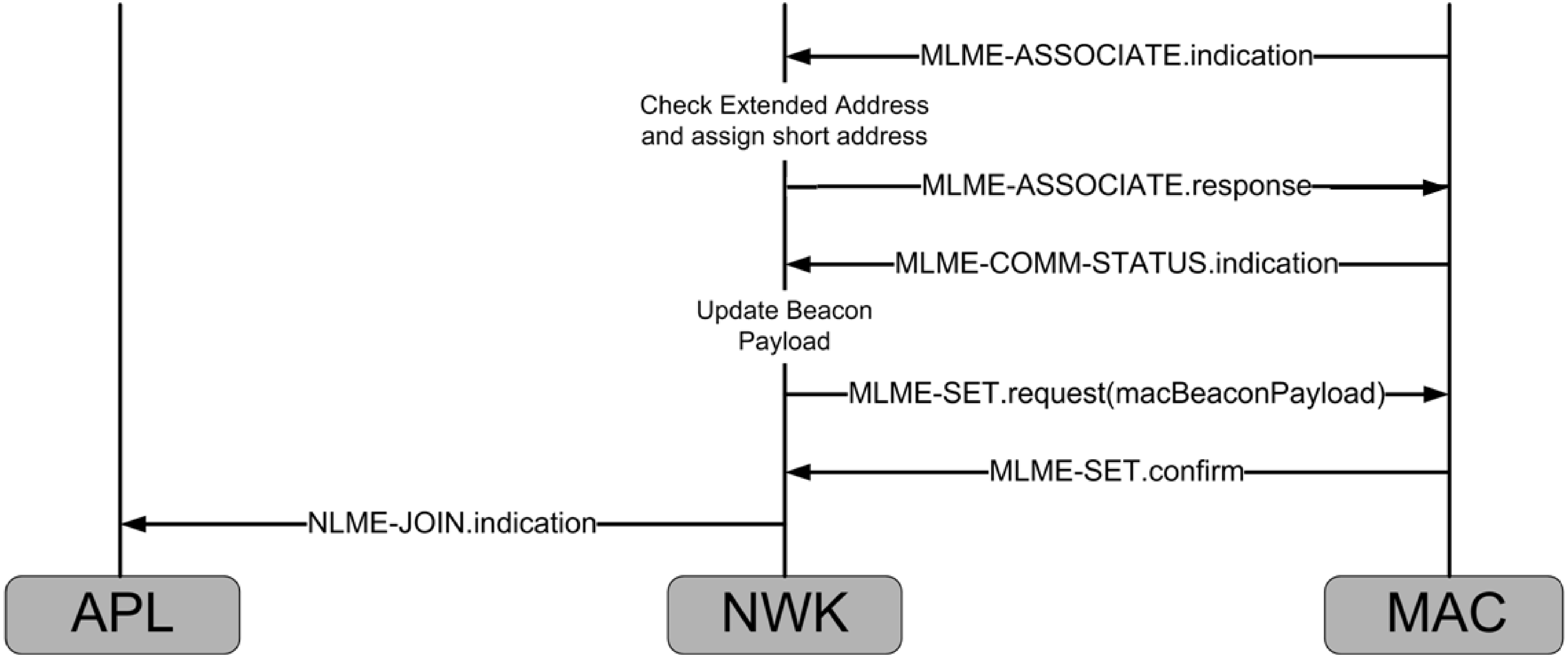
Maintenance of the network and the devices

- Join through association: Child procedure



Maintenance of the network and the devices

- Join through association: Parent procedure



Maintenance of the network and the devices

- Leave the network: NLME-LEAVE.request
- Own choice to leave the network
  - ZigBee Co-ordinator or ZigBee Router
    - Send Leave command frame
    - Both children as parent should be informed
    - Force children to leave the network
  - ZigBee End Device
    - Send Leave command frame
    - Inform the parent device
- Force others to leave the network

Maintenance of the network and the devices

- Neighbour tables
  - Store information of all devices within transmission range
  - Neighbour table entry for each neighbour:

Field name	***Description***
Extended Address	64-bit IEEE address which is unique for each device
Network Address	16-bit network address
Device Type	Type of ZigBee device: ZED, ZR, ZC
RxOnWhenIdle	Is the receiver working during its idle period
Incoming Beacon Timestamp	The moment when the last beacon frame was received from its neighbour

  - Neighbour routing
  - Network Discovery

Maintenance of the network and the devices

- Address assignment
  - 16-bit network address
  - Unique in the network
  - Default 0x00 => reserved for ZC of the network
  - Distributed method
  - Stochastic method

- Distributed address assignment
  - Structured method
  - ZED obtains 1 network address
  - Each possible parent (ZC of ZR) obtains a sub-bloc of addresses
  - Size of the sub-bloc depends on depth in the network
  - For good functioning: add some restrictions to the network

Maintenance of the network and the devices

- Distributed address assignment
  - Restrictions chosen by the ZC at start-up of the network
    - *Cm* : maximum number of children a device is allowed to have
    - *Rm* : maximum number of children which may have routing capacities
    - *Lm* : maximum depth of the network
  - ‘depth’ (*d*) of a device:
    - minimum number of hops towards the ZC
    - ZC has *d* = 0
  - Cskip(*d*)-function calculates the size of the sub-bloc of addresses available for a ZC or ZR at ‘depth’ *d*.

$$Cskip(d) = \begin{cases} 1 + Cm - d - 1, if \;\; Rm = 1 \\ \dfrac{1 + Cm - Rm - Cm.Rm^{Lm-d-1}}{1 - Rm}, otherwise \end{cases}$$

Maintenance of the network and the devices

- Distributed address assignment
  - Cskip(d)-value = 0 : device can not have children
  - Cskip(d)-value > 0 : device can have children

  - Distribution of the network addresses
    - ZR: 1st: $A = A_{parent} + 1$

      2nd : $A = A_{parent} + Cskip(d) + 1$

      d is the 'depth' of the parent device
    - ZED: n-th device:

$$A_n = A_{parent} + Cskip(d).Rm + n$$

Maintenance of the network and the devices

- Distributed address assignment: example

Parameter	***Value***
Cm	8
Rm	4
Lm	3

Depth in the Network, d	***Offset Value, Cskip(d)***
0	31
1	7
2	1
3	0

Maintenance of the network and the devices

- Distributed address assignment: example

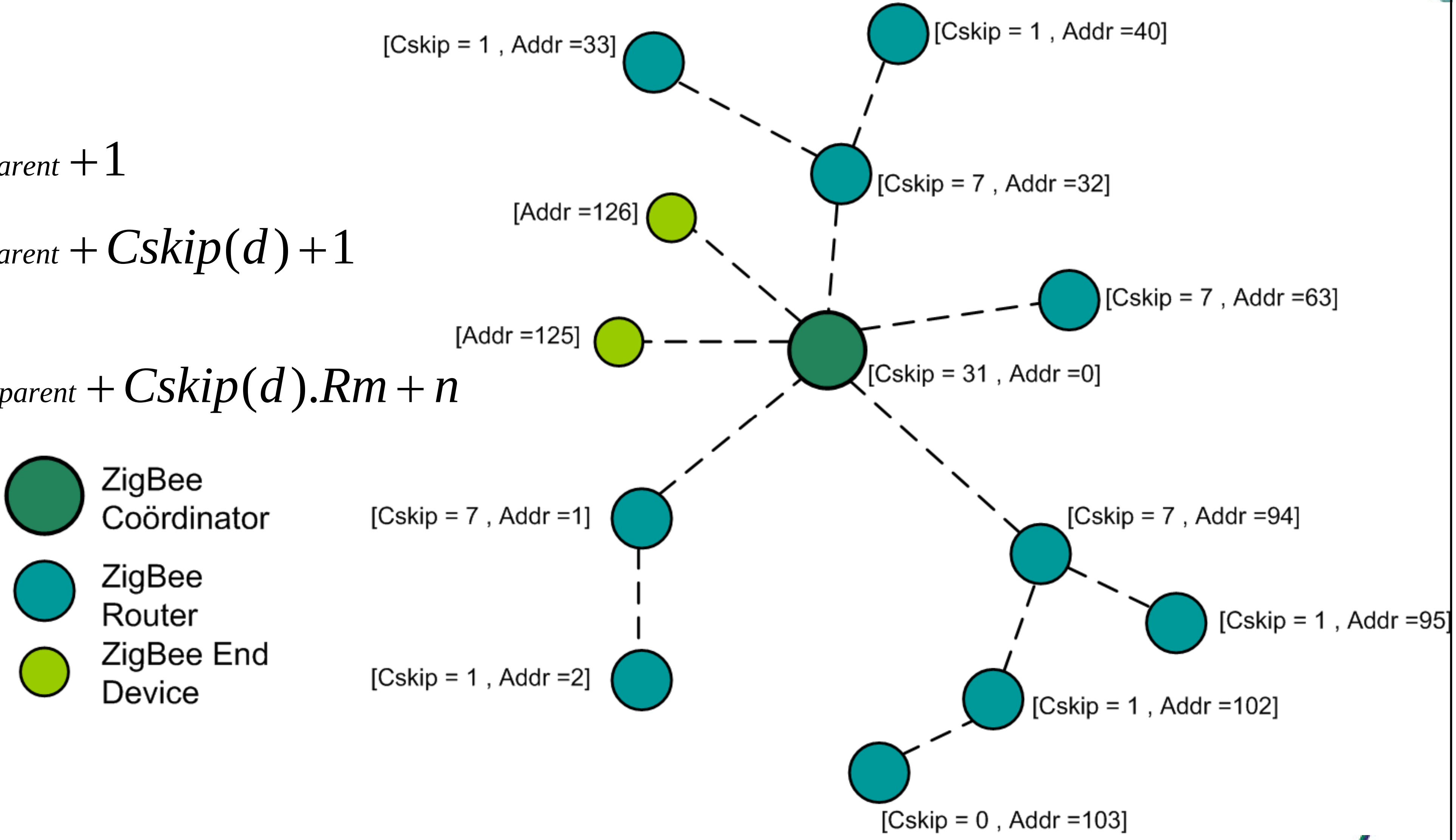
ZR:

$$A = A_{parent} + 1$$

$$A = A_{parent} + Cskip(d) + 1$$

ZED:

$$A_n = A_{parent} + Cskip(d).Rm + n$$



Maintenance of the network and the devices

- Stochastic address assignment
  - Not structured
  - Parent grants an at random chosen address to its child
  - Restrictions:
    - Never granted the address before
    - Address not present in its neighbour table
  - Disadvantage:
    - Conflicts with other devices can occur
    - Search for conflicts and correct them

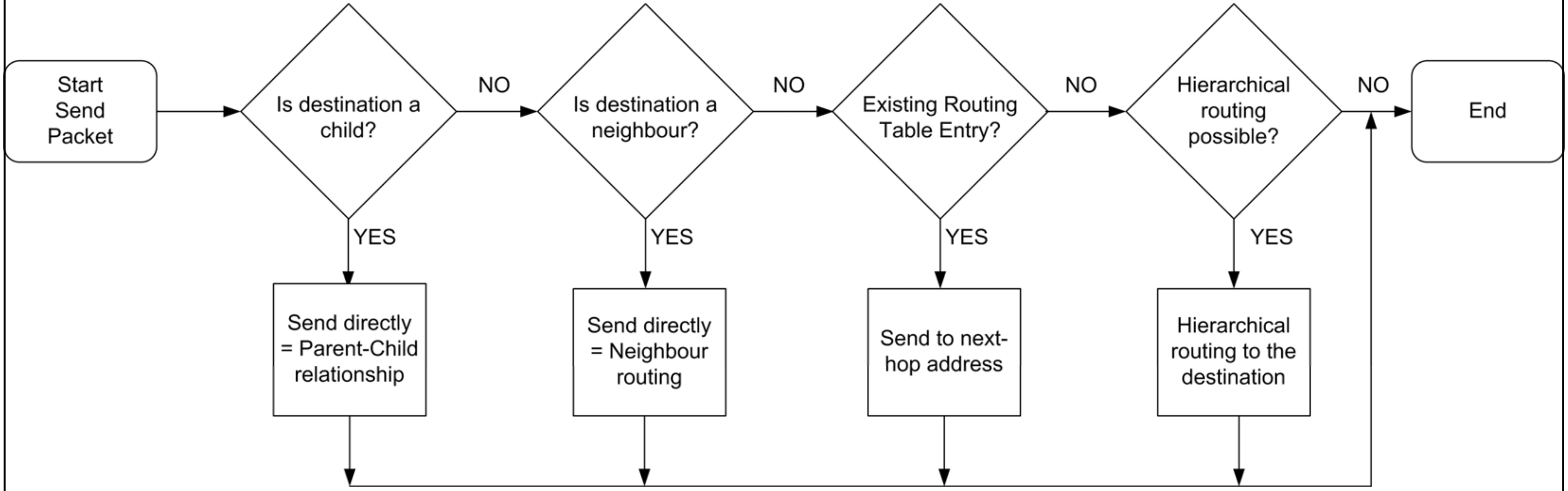
Routing

- Routing of packets from the source to the destination
- Routing Cost:
  - Take a cost into account for each hop
  - Compare different routes
  - Discover route through Route Discovery
  - Used to compose Routing Tables
- Routing Tables:
  - Only for ZR en ZC
  - For each destination a Routing Table Entry

Field Name	***Description***
Destination Address	16-bit network address of the device
Status	Status of the route: Active, Not Active, …
Next-hop Address	16-bit network address of the next-hop device on the route to the destination

Routing

- Routing mechanism


Start Send Packet
Is destination a child?
NO
Is destination a neighbour?
NO
Existing Routing Table Entry?
NO
Hierarchical routing possible?
NO
End
YES
Send directly = Parent-Child relationship
YES
Send directly = Neighbour routing
YES
Send to next-hop address
YES
Hierarchical routing to the destination

Routing

- Hierarchical routing
  - Uses the distributed address assignment
  - Is the destination a descendant?

    = child, grandchild or great-grandchild

  ⇒ Pass message to appropriate child

  - Is destination not a descendant?

  ⇒ Pass message to parent

Routing

- Hierarchical routing
  - Decide if the destination is a descendant or not
    - *A* = Own address
    - *D* = Destination address

$$A < D < A + Cskip(d-1)$$

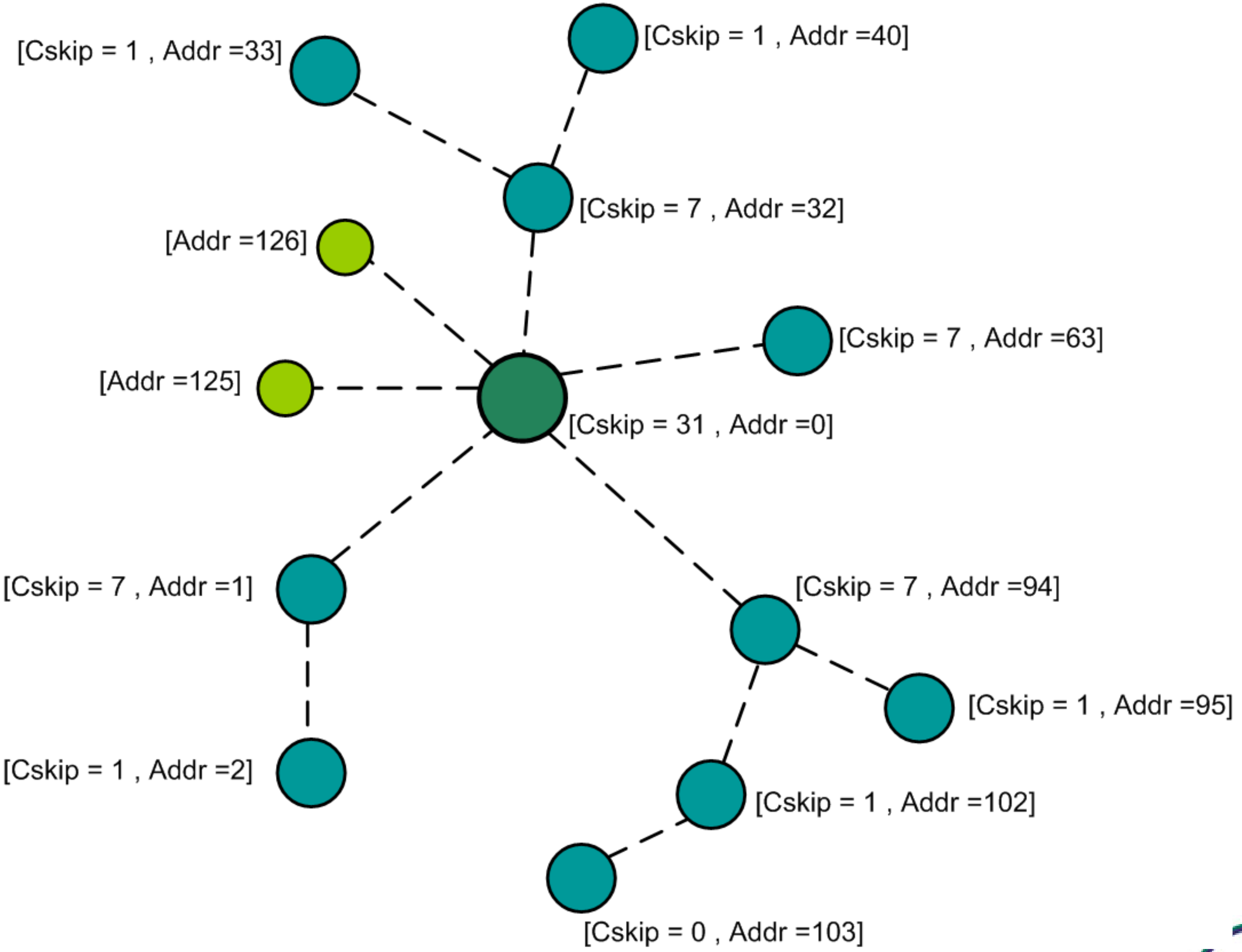
  - What is the next-hop address (*N*)?

$$N = A + 1 + \left\lfloor \frac{D-(A+1)}{Cskip(d)} \right\rfloor .Cskip(d)$$

Routing

- Hierarchical routing: example

Device 94 (A)
with *d* = 1
transmits
a packet to
device 103 (D)



Routing

- Hierarchical routing: example: *A* = 94, *d* = 1, *D* = 103
- Is the destination a descendant?

$$A < D < A + Cskip(d-1) \qquad 94 < 103 < 94 + 31$$

- What is the next-hop address?

$$N = A + 1 + \left\lfloor \frac{D-(A+1)}{Cskip(d)} \right\rfloor . Cskip(d)$$

$$N = 94 + 1 + \left\lfloor \frac{103-(94+1)}{7} \right\rfloor . 7 = 102$$

Depth in the Network, d	***Offset Value, Cskip(d)***
0	31
1	7
2	1
3	0

ZigBee – Application Layer (APL)

Anneleen Van Nieuwenhuyse

KaHo Sint-Lieven - DraMCo – 21/5/2009

Overview

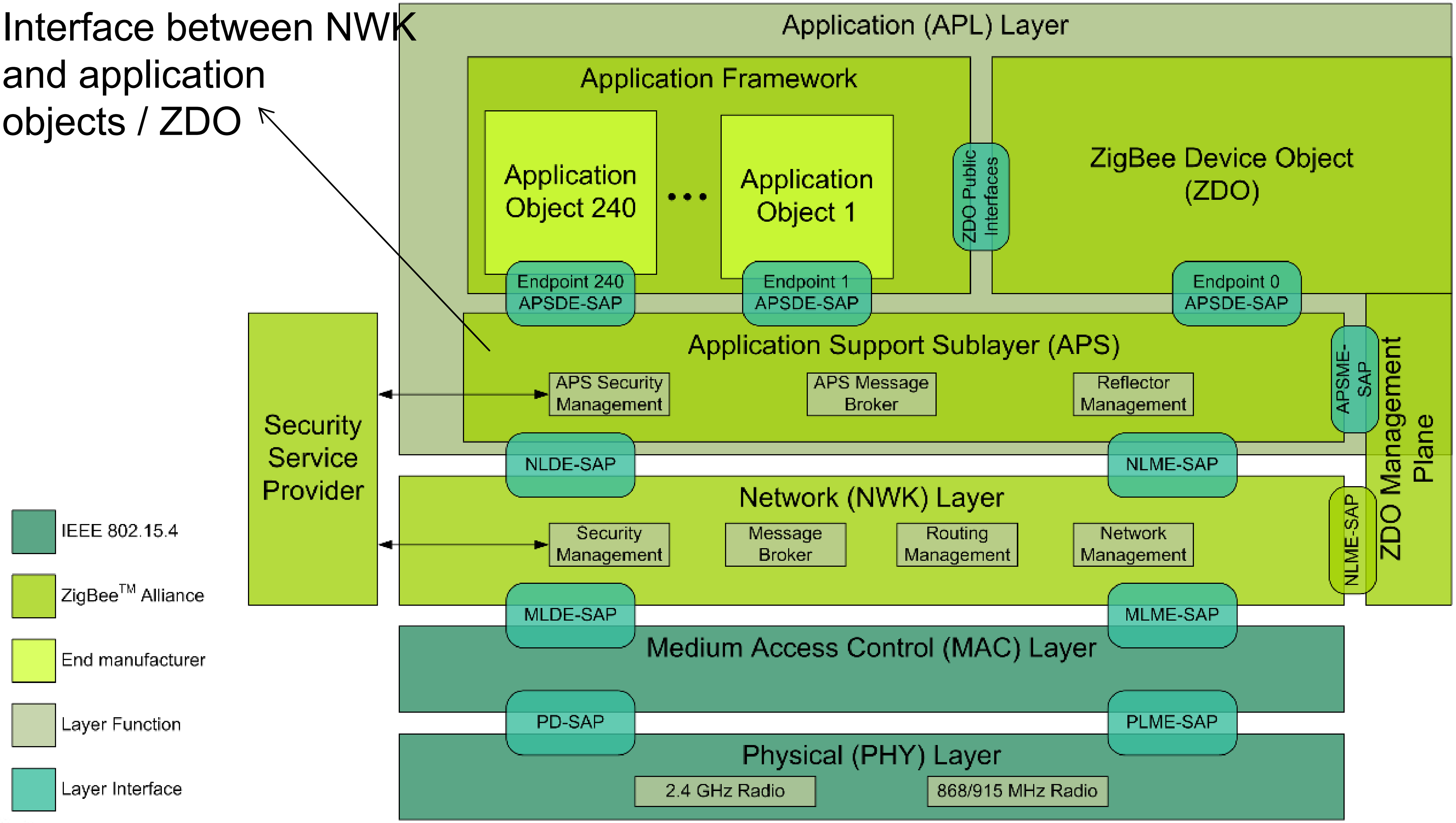
- Introduction
- Application Support Sub-layer (APS)
- Application Framework (AF)
- ZigBee Device Objects (ZDO)
- Commissioning

APL: general

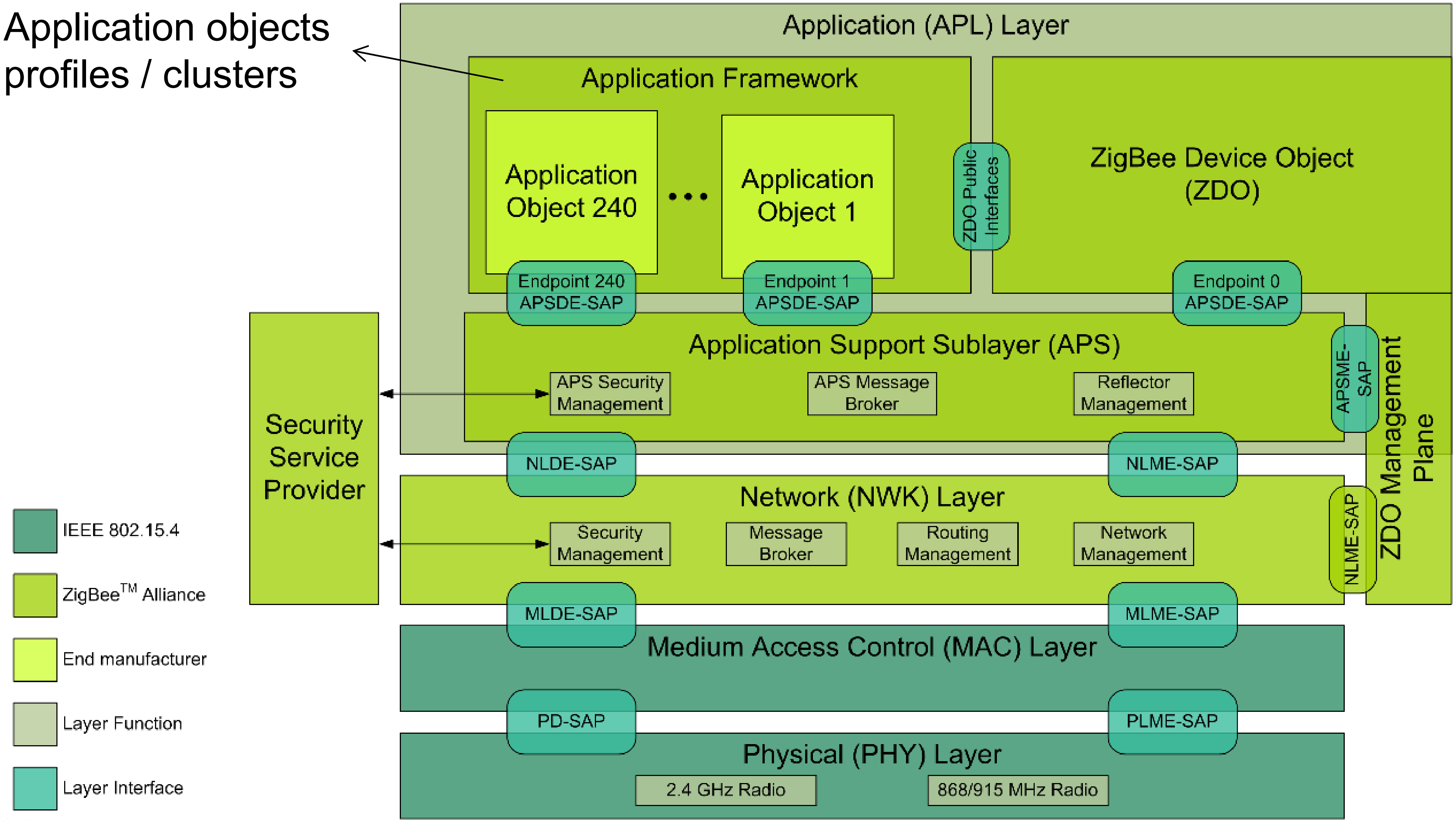
- Lower layers
  - transport
  - connections
  - network
- The exact application field is situated in the Application layer
  - What does the node do? (ex. Measure temperature)
  - which type of node (ZC, ZR, ZED)
  - ZigBee functionality
    - groups
    - binding
    - profiles
- Is the closest to the user

ZigBee Protocol stack

Interface between NWK and application objects / ZDO



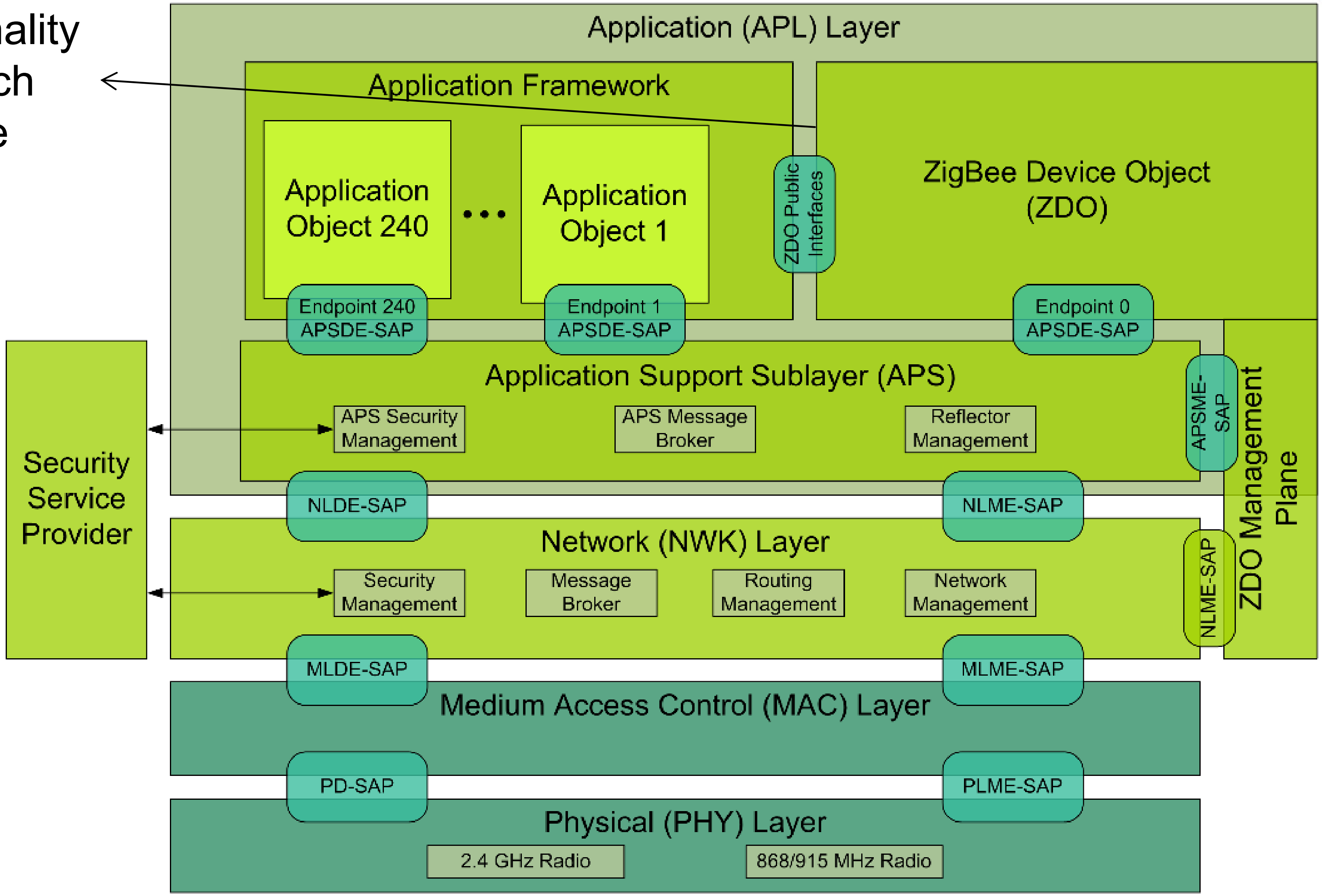
ZigBee Protocol stack



Application objects
profiles / clusters

ZigBee Protocol stack

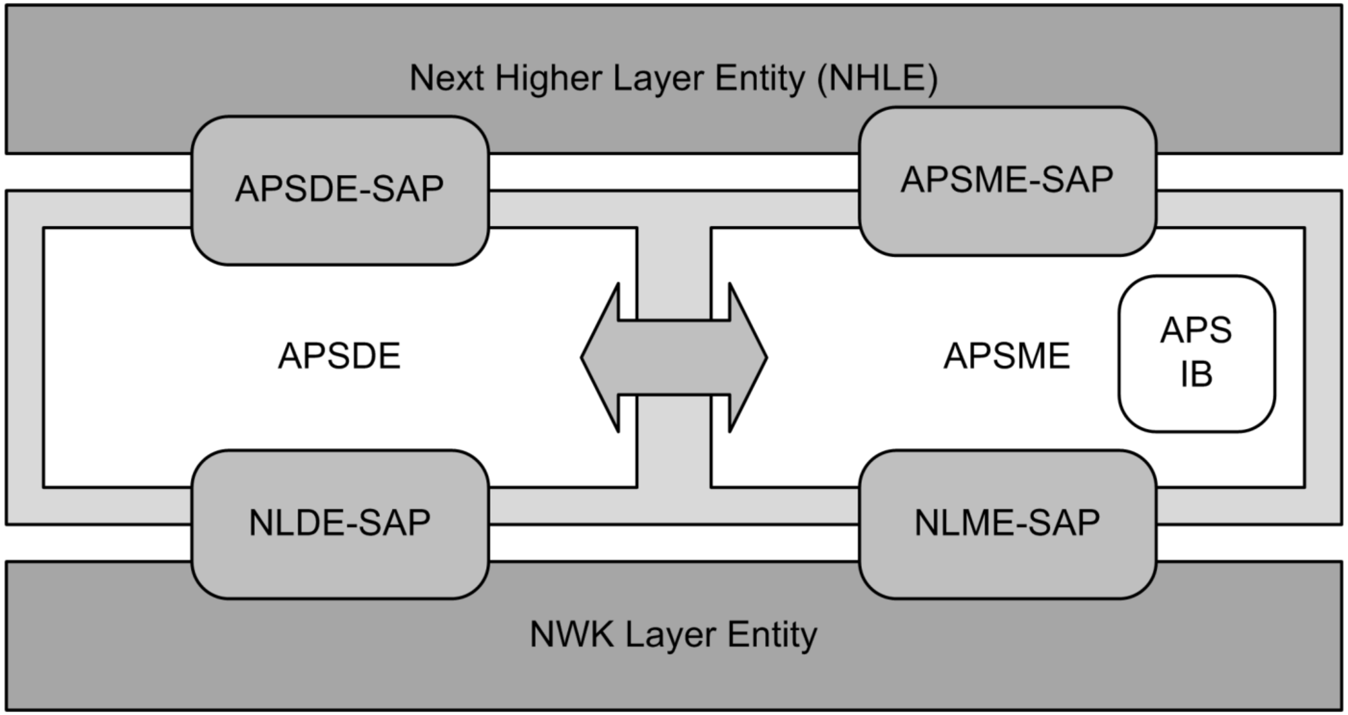
Basic functionality
Present in each
ZigBee device



🟩	IEEE 802.15.4
🟩	ZigBee^{TM} Alliance
🟨	End manufacturer
▨	Layer Function
🟩	Layer Interface

APS: Overview

- 2 Service Entities (Data & Management)
- Service Access points



APS: Data Entity

- Data transport between two devices (HLE)
  - Application Objects
  - ZDO
  - Groups
- End-to-end retries (confidentiality)
- Fragmentation
- Elimination of duplicates

APS: Data Entity

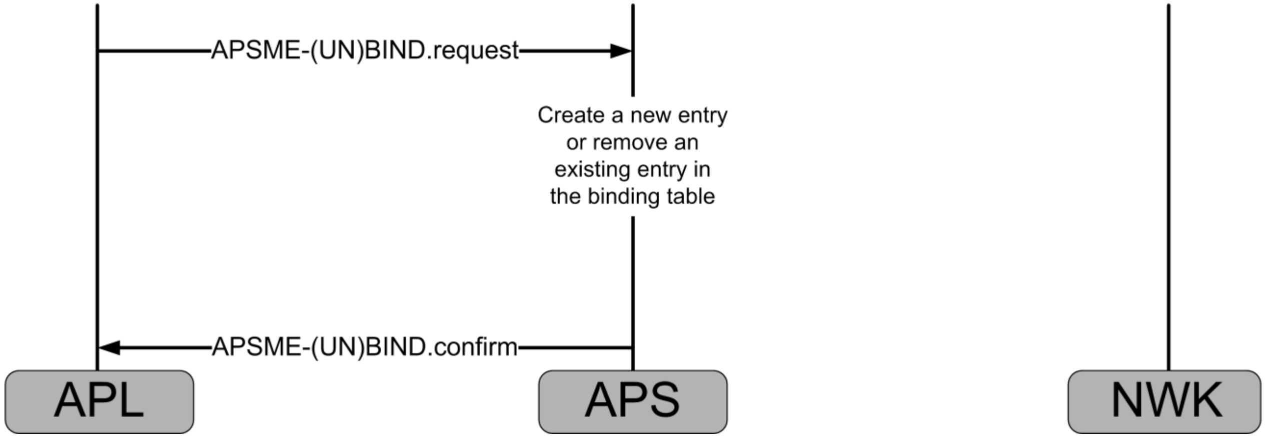
- APSDE-DATA primitives
  - Request: request to send data
    - Addressing methods
    - Security
    - Fragmentation
    - Max. # hops
  - Confirm: result of the request
  - Indication: reception of data

APS: Management Entity

- Communication of ZDO (and Application Objects) with the stack
- Offers “ZigBee functionality”
  - Binding
  - AIB
  - Group management
  - Authenticated relationships

APS: Management Entity

- APSME-BIND primitive
  - Request: Ask to ‘bind’ two devices (can also be groups)
  - Confirm: results of the request
- APSME-UNBIND primitive
  - Request: ask to ‘un-bind’ the devices (delete entry)
  - Confirm: result of the request
- Binding table


APSME-(UN)BIND.request
Create a new entry or remove an existing entry in the binding table
APSME-(UN)BIND.confirm
APL
APS
NWK

APS: Management Entity

- APSME-ADD-GROUP primitive
  - Request: add endpoints to a group
  - Confirm: results of the request
- APSME-REMOVE-GROUP primitive
  - Request: delete endpoint out of the group
  - Confirm: result of the request
- APSME-REMOVE-ALL-GROUPS

APS: Management Entity

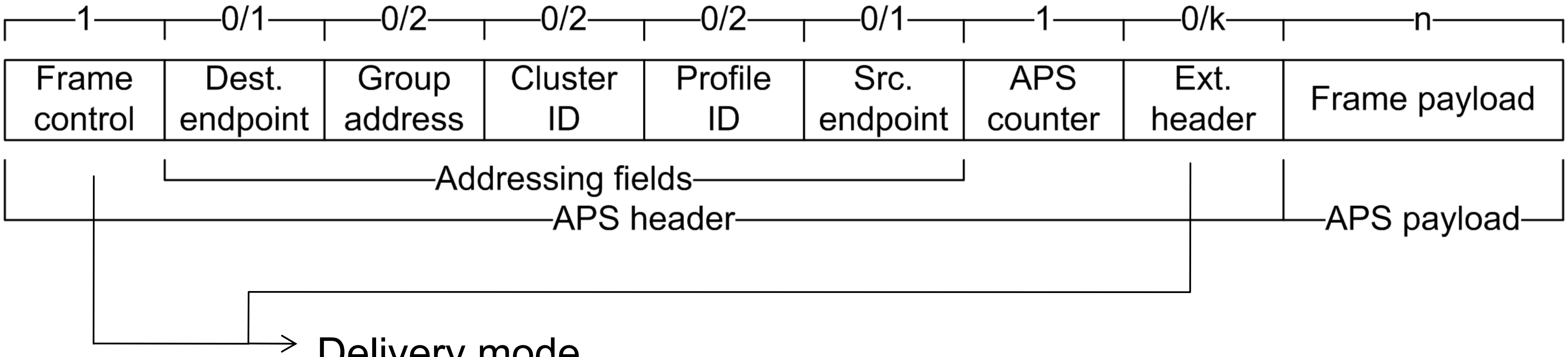
- APSME-GET primitive
  - Request: read an attribute out of the AIB
  - Confirm: results of the request
- APSME-SET primitive
  - Request: writing an attribute to the AIB
  - Confirm: results of the request

APS: Management Entity

- Persistent data
  - Binding table
  - Group table
  - Descriptors (node, node power, simple)
  - FLASH, EEPROM, …

APS: Frame format

- APS frame = NWK payload
- Is composed by the APS
  - primitive
  - arguments



1	0/1	0/2	0/2	0/2	0/1	1	0/k	n
Frame control	Dest. endpoint	Group address	Cluster ID	Profile ID	Src. endpoint	APS counter	Ext. header	Frame payload

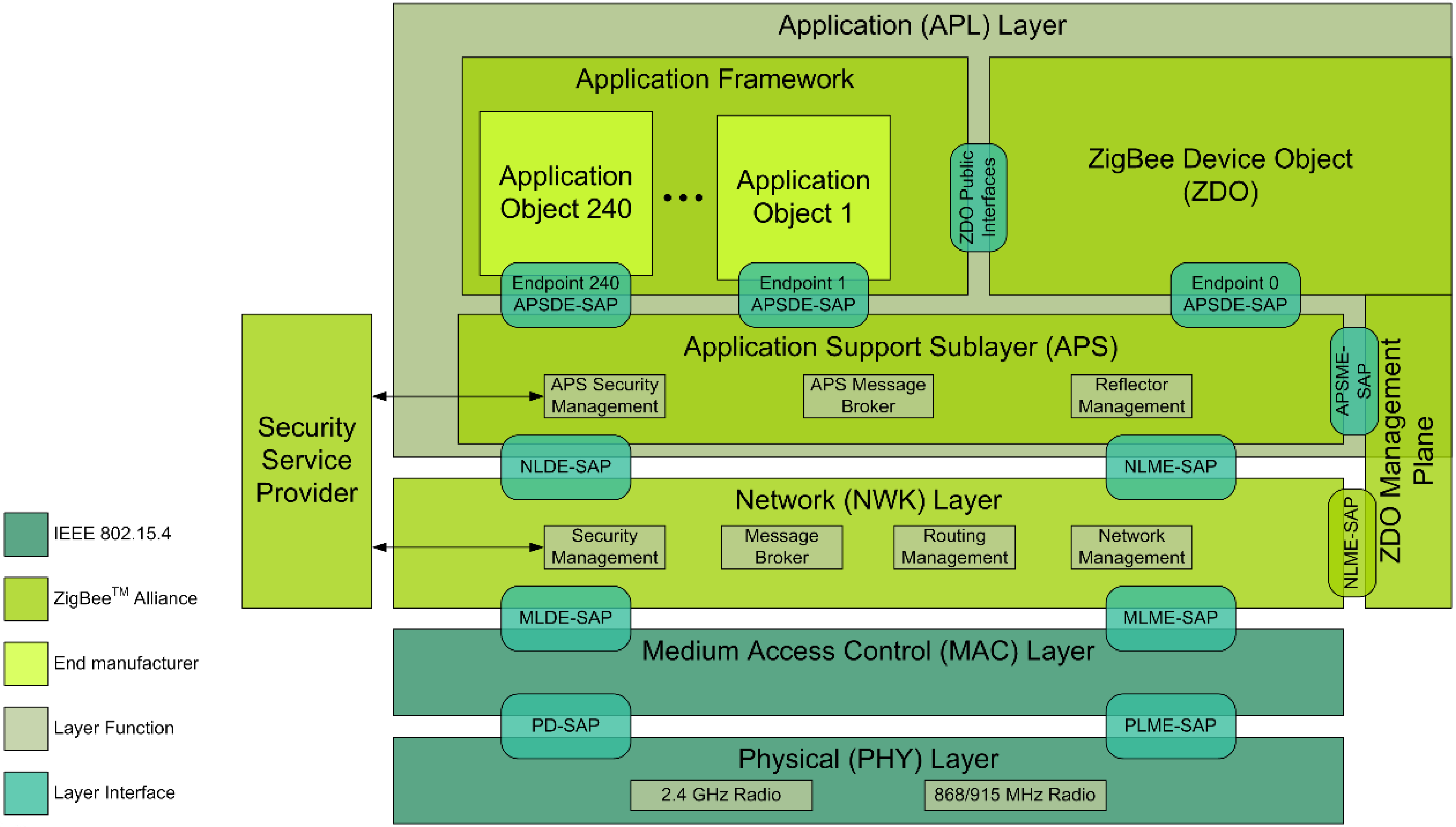
Addressing fields

APS header

APS payload

Delivery mode
ACK necessary
Extended header?

ZigBee Protocol stack

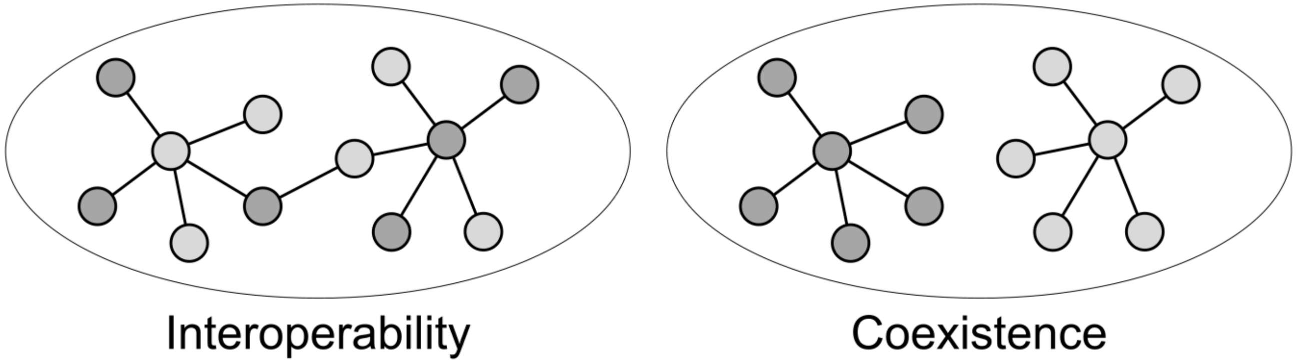


Application Framework

- Profiles
  - Standard messages for certain applications (Ex. Home Automation)
  - Clusters
  - Descriptors
- Application Objects
  - Endpoints
    - 0x00: ZDO
    - 0x01 – 0xf0: user
    - 0xf1 – 0xfe: reserved
    - 0xff: broadcast
  - The application

Profiles

- Collect devices and messages
  - Profile ID
  - ex. Lamp and switch
- Public
  - Interoperability (ZigBee compliance)
- Private
  - Product differentiation
  - New applications (No public profile available)
  - Co-existence



Profiles

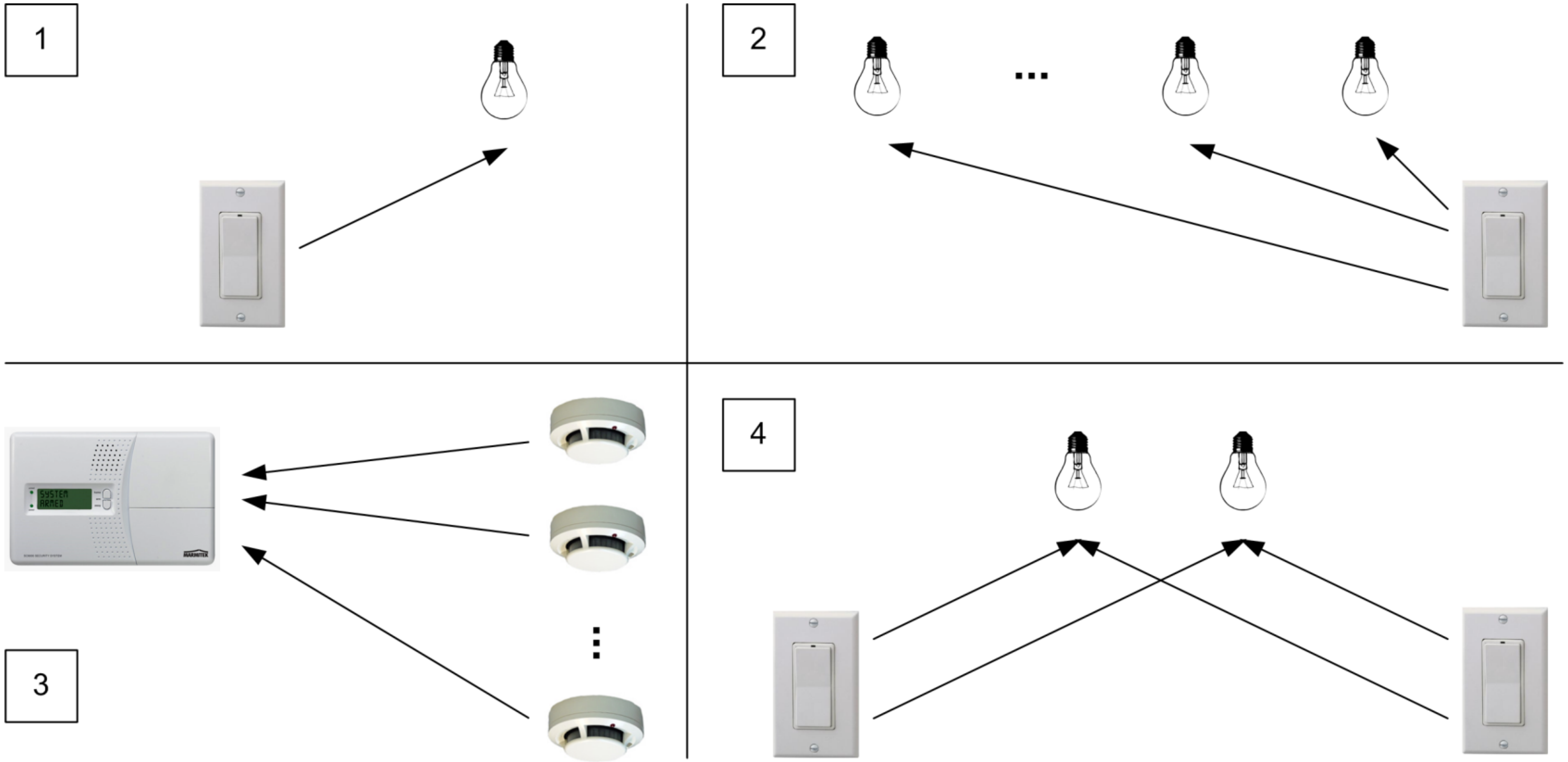
- Home Automation
  - Flexible management of lighting, heating, airco
- Smart Energy
  - Energy saving
- Building Automation
  - Home Automation for public buildings (security)

ZigBee Cluster Library

- Library with standard clusters
  - Functional domains (lighting, HVAC, …)
- Profiles can be based on ZCL
  - Reuse of similar clusters
  - ex: lighting (Home Automation en Building Automation)

ZigBee Cluster Library

- Binding relations
  1. One-to-one
  2. One-to-many
  3. Many-to-one
  4. Many-to-many



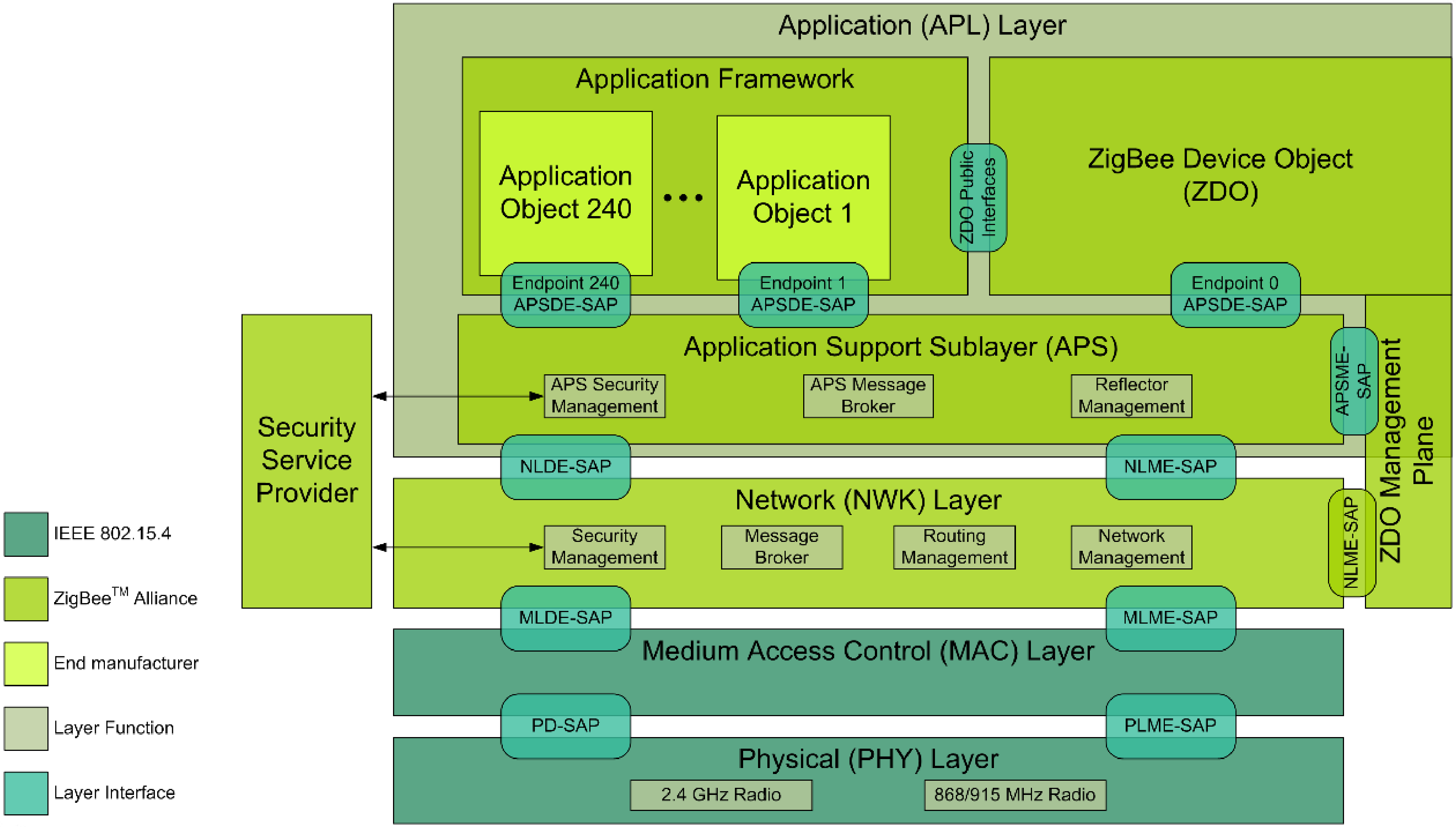
Descriptors

- Node descriptor
  - Type node
  - Complex and/or user descriptor
  - TC, discovery cache, binding cache
- Node power descriptor
  - Energy source
  - Available energy
- Simple descriptor
  - For each endpoint
  - Used profile and clusters
- Complex descriptor
  - Optional
  - Serial number
  - Manufacturer
  - Charactar set
  - …
- User descriptor
  - Optional
  - “readable” naam
  - Ex. “Heating Liv.”

ZigBee Device Profile

- One profile
- Used by ZDO
- For all ZigBee devices
- The “ZigBee-functionality”
  - Device and service discovery
  - Binding functionality
  - Network management

ZigBee Protocol stack



ZigBee Device Objects (general)

- Offer several services
- Depending of the type of the devices
- Mandatory vs. optional
- Initialize APS
- Collect and reassembling of configuration-information concerning the end-application so the services can be offered correctly

Device en Service Discovery

- Primary Discovery Cache → “advertised” in descriptor
- Device discovery
  - Retrieve addresses
- Service discovery
  - By the use of the descriptors (underlying profile, used clusters, active endpoints,…)
- Device and service discovery should be supported by all nodes

Network manager

- Implementation of type node ZC, ZR of ZED
- ZR en ZED:
  - Node can (re-) join the network
- ZC en ZR:
  - Start-up of new networks
- Detection of interference

Security Manager

Binding Manager

- Deal with binding-related request
- Help with commissioning

Node manager

- Remote management commands
  - Retrieve information (vb. Routing table)
  - Allow or reject joining the network
  - Start network discovery

Group manager

- Deal with “group-related” requests