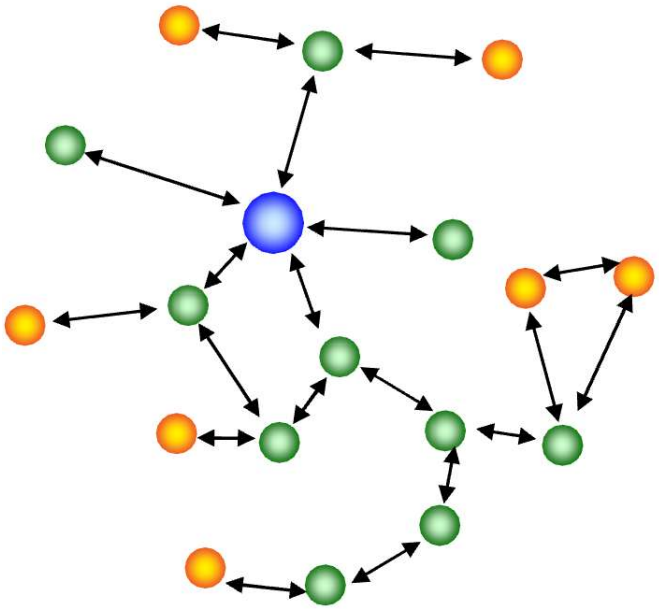
Žilinská univerzita v Žiline
Fakulta riadenia a informatiky
Katedra technickej kybernetiky

Štandard IEEE 802.15.4



Ondrej Karpiš

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

IEEE 802.x

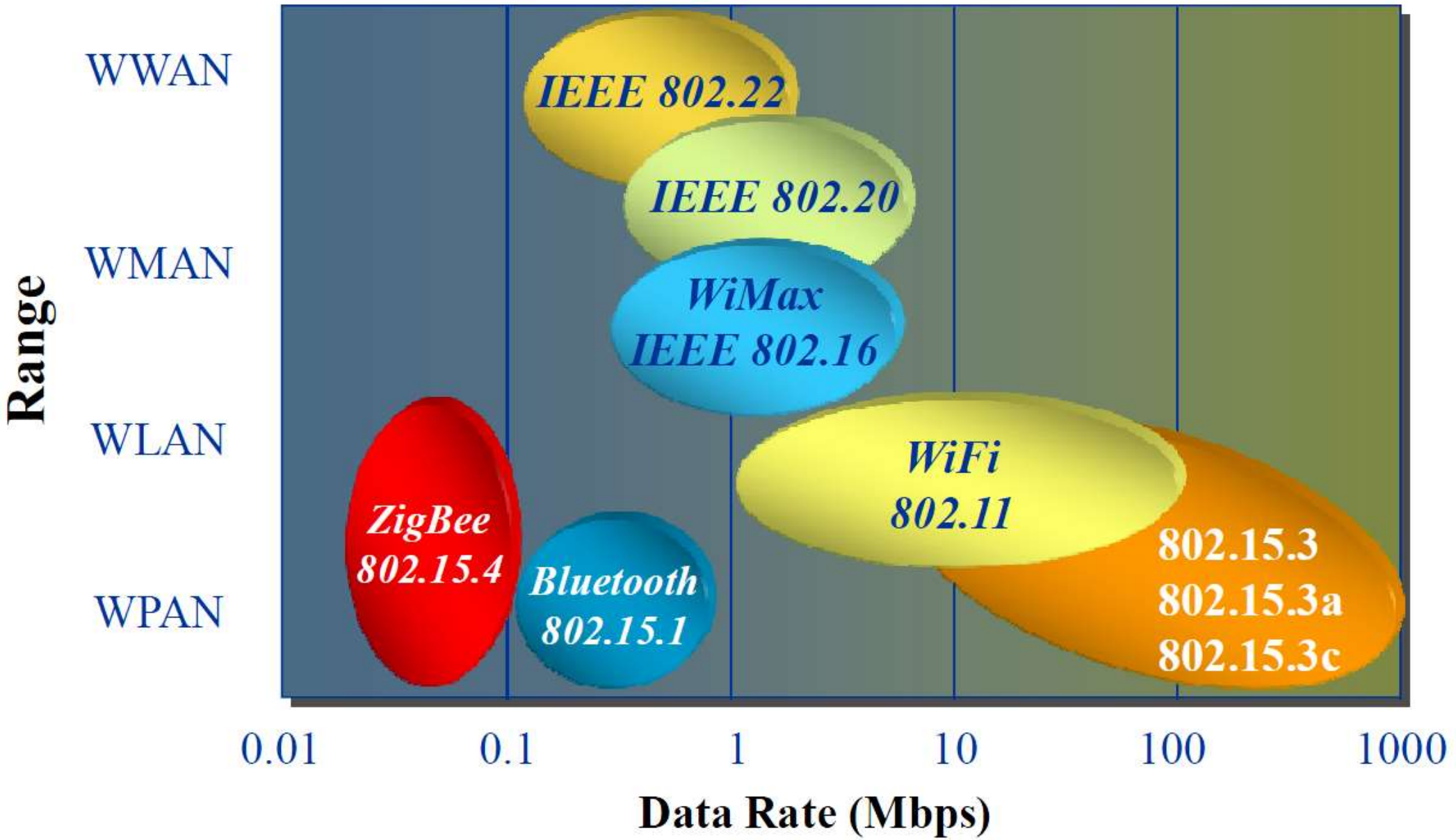
- 802 – rodina štandardov pre LAN a MAN
  – len fyzická (PHY) a linková vrstva (LLC a MAC)

- 802.3 – Ethernet
- 802.4 – Token Bus
- 802.11 (a/b/g/n) – WiFi
- 802.15 – Wireless PAN (Personal Area Network)

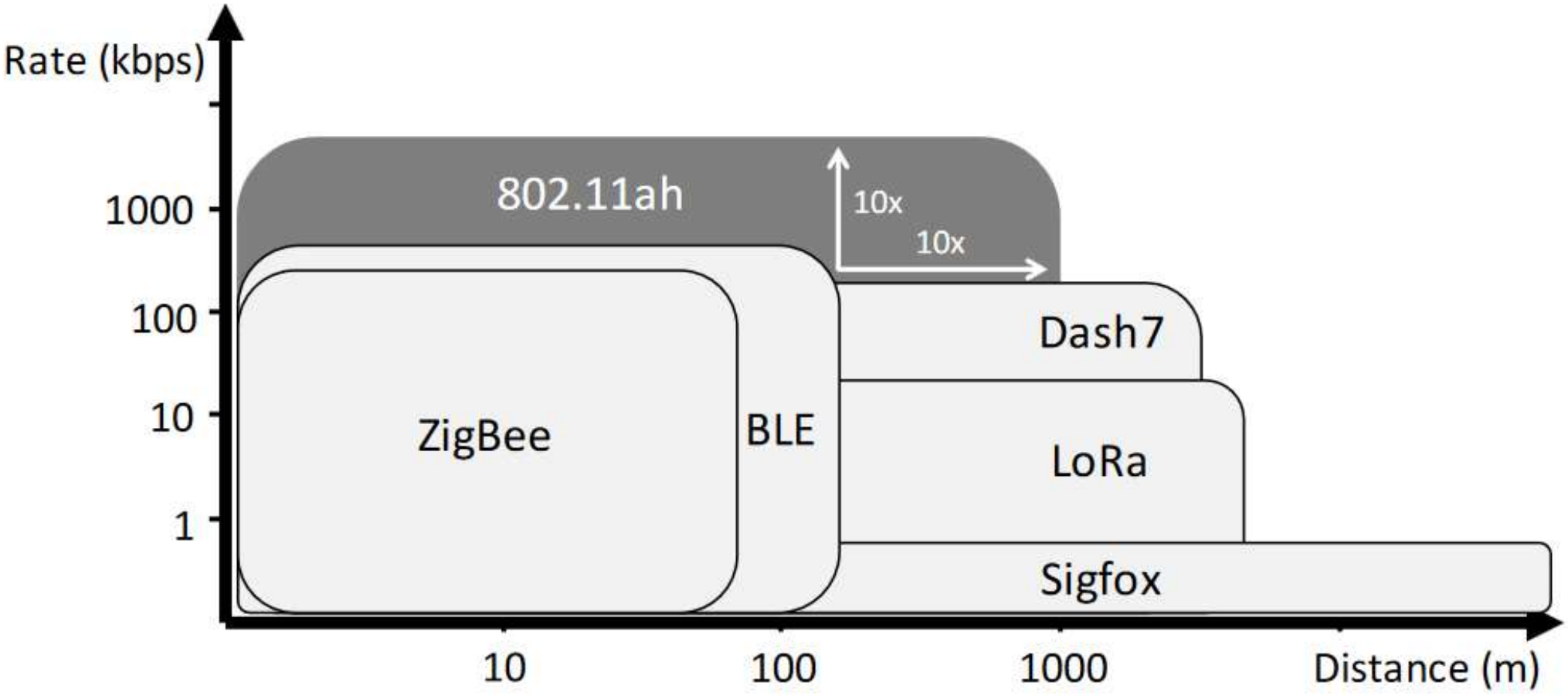
IEEE 802.15

- 802.15.1 – Bluetooth
- 802.15.3 – High-Rate wireless PAN
- 802.15.4 – Low-Rate wireless PAN (LR-WPAN) (ZigBee, WirelessHART, MiWi, ISA100.11a, 6LoWPAN, Thread, SNAP)
- 802.15.6 – Body area network (BAN)

Bezdrôtové štandardy (2005)



Bezdrôtové štandardy – súčasnosť



Verzie 802.15.4

802.15.4-2003 – pôvodná verzia (2 PHY)

802.15.4-2006 – 2 nové PHY, úprava MAC

802.15.4-2011 a dodatky

- nové PHY: Čína a Japonsko, RFID, Medical Body Area Network – MBAN
- ranging, channel hopping (MAC)

Verzie 802.15.4

802.15.4-2015

- PHY: smart utility networks (SUNs), television white space (TVWS) operation, low-energy critical infrastructure monitoring (LECIM), rail communications and control (RCC)
- channel agility, low-energy mechanisms, enhanced acknowledgment with secured data, prioritized channel access

Verzie 802.15.4

802.15.4-2020

- nové PHY: China medical band – CMB
- modulácia, kódovanie:
  - ternary amplitude shift keying (TASK)
  - rate switch Gaussian frequency shift keying (RS-GFSK)

PHY [MHz]	Freq. [MHz]	Modulation	Bit rate [kb/s]	Symbol rate [ksymbol/s]	Chip rate [kchips/s]
780	779-787	O-QPSK, MPSK	250	62.5	1000
868/915	868-868.6 902-928	BPSK	20 40	20 40	300 600
868/915 (optional)	868-868.6 902-928	ASK (PSSS), O-QPSK	100, 250	12.5, 25, 50, 62.5	400, 1000, 1600
950	950-956	GFSK	100	100	-
950	950-956	BPSK	20	20	300
2450 DSSS	2400-2483.5	O-QPSK	250	62.5	2000
2450 CSS (optional)	2400-2483.5	DQPSK	250, 1000	167	
UWB (optional)	250-750 3244-4742 5944-10234	BPM-BPSK	110, 850, 1700, 6810, 27240		

Prenosové kanály

Stránka 0 (802.15.4-2003):

- 868 MHz – 1 kanál (Európa)

  Fc = 868.3 MHz, k = 0

- 915 MHz – 10 kanálov (USA a Austrália)

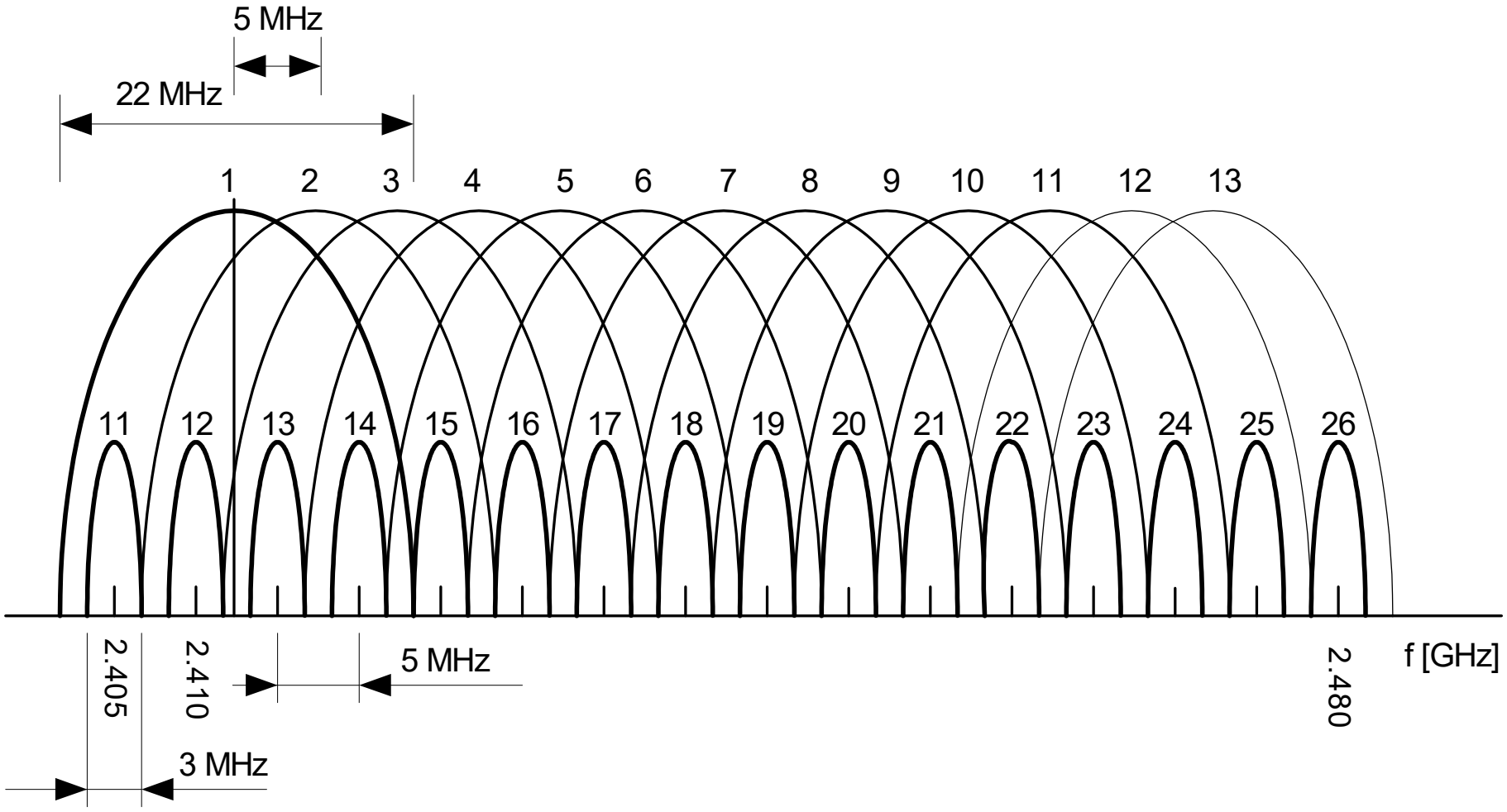
  Fc = 906 + 2.(k-1) [MHz], k = 1, 2 … 10

- 2450 MHz – 16 kanálov (celý svet)

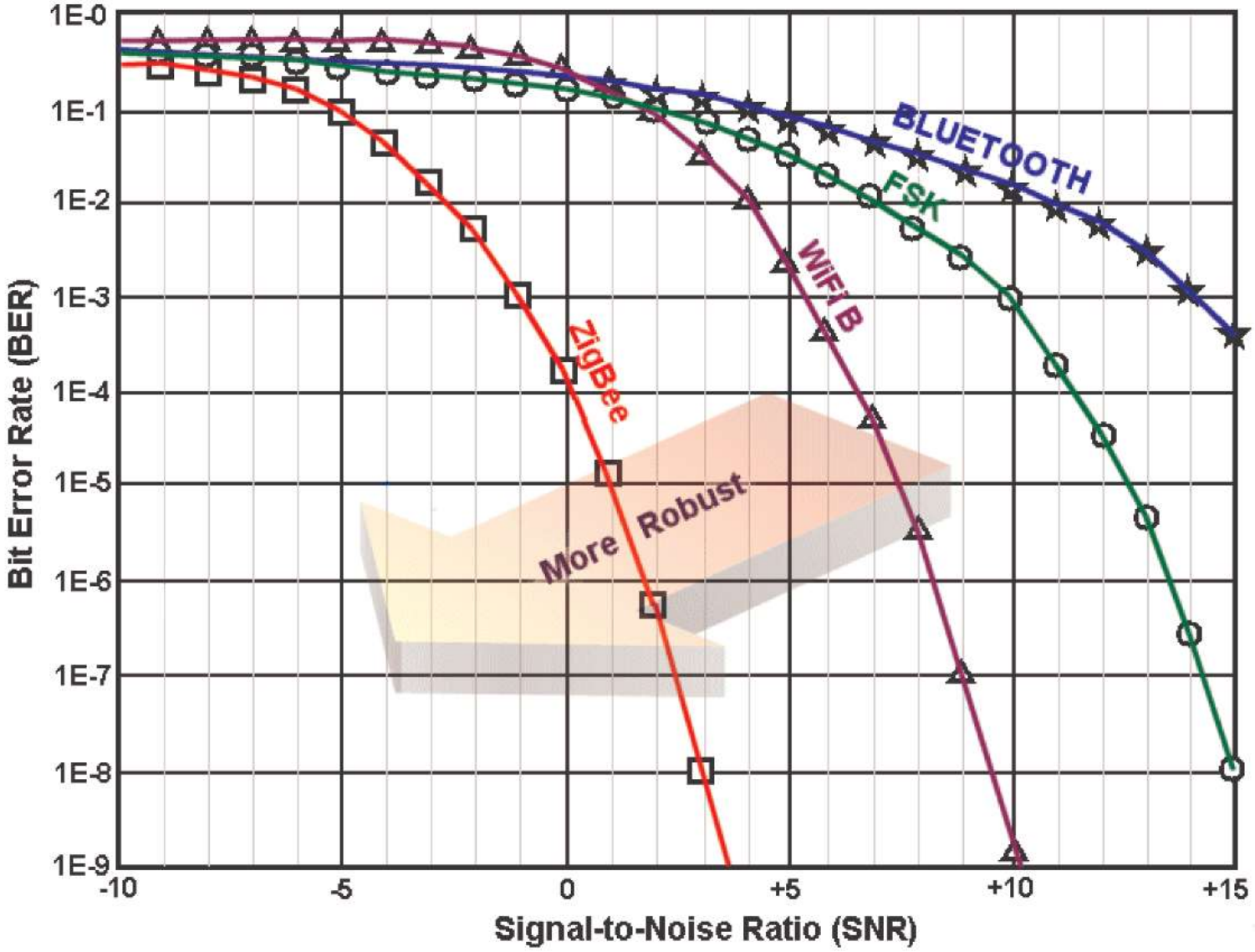
  Fc = 2405 + 5.(k-11) [MHz], k = 11, 12 … 26

Fc – centrálna frekvencia, k – číslo kanála

Kanály pre 802.11.b a 802.15.4



Porovnanie štandardov pre 2.4 GHz



IEEE 802.15.4 – hlavné ciele

- jednoduchá inštalácia
- spoľahlivý prenos
- extrémne nízke náklady
- značná životnosť batérií
- jednoduchý a flexibilný protokol

IEEE 802.15.4 – vlastnosti

- topológia hviezda alebo peer-to-peer
- max. 2^{16} zariadení v sieti (16b a 64b adresa)
- možnosť alokácie prenosového pásma (TDMA)
- prístupová metóda CSMA-CA, ALOHA
- spoľahlivý prenos
- bezpečná komunikácia
- detekcia energie (ED)
- indikácia kvality linky (LQI)

IEEE 802.15.4 – aplikácie

- Automatizácia domácností
- Priemyselná automatizácia
- Vzdialené meranie
- Interaktívne hračky
- Sledovanie polohy
- Zdravotníctvo
- Životné prostredie
- Poľnohospodárstvo
- …

Typy zariadení

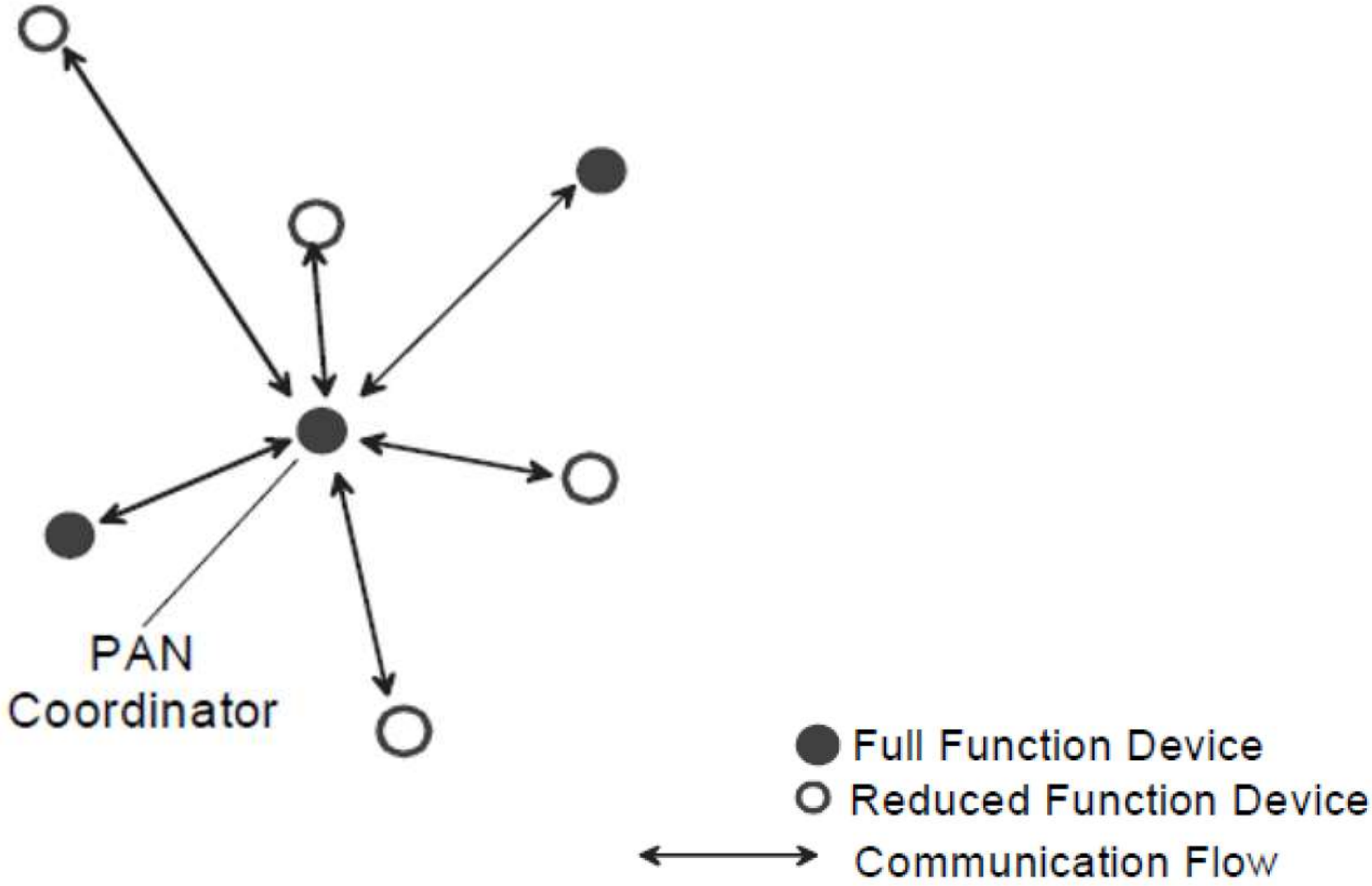
Fyzické zariadenia

- FFD – Full-function Device
- RFD – Reduced-function Device

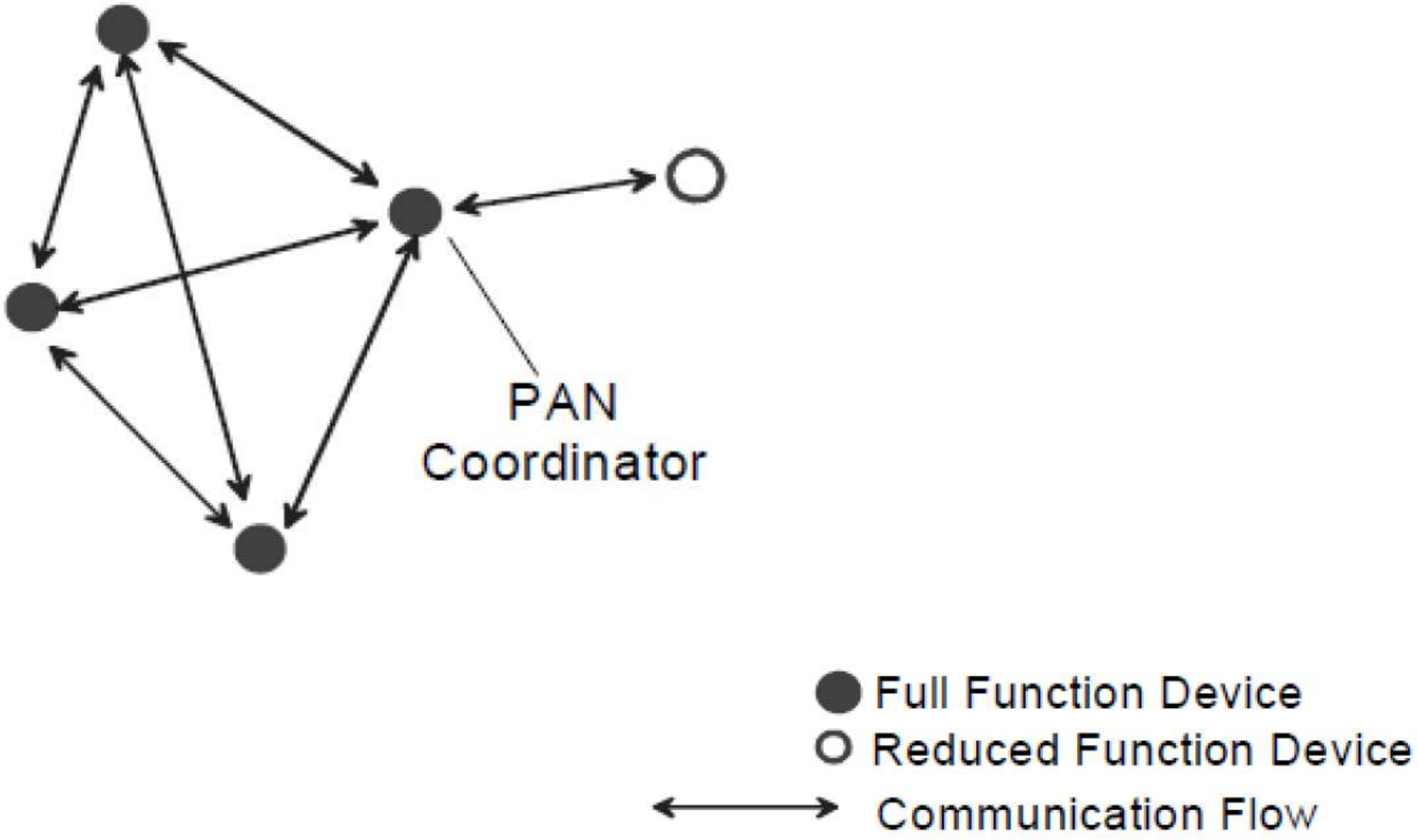
Logické zariadenia

- PAN koordinátor (FFD)
- Koordinátor (FFD)
- Zariadenie (device) (RFD, FFD)

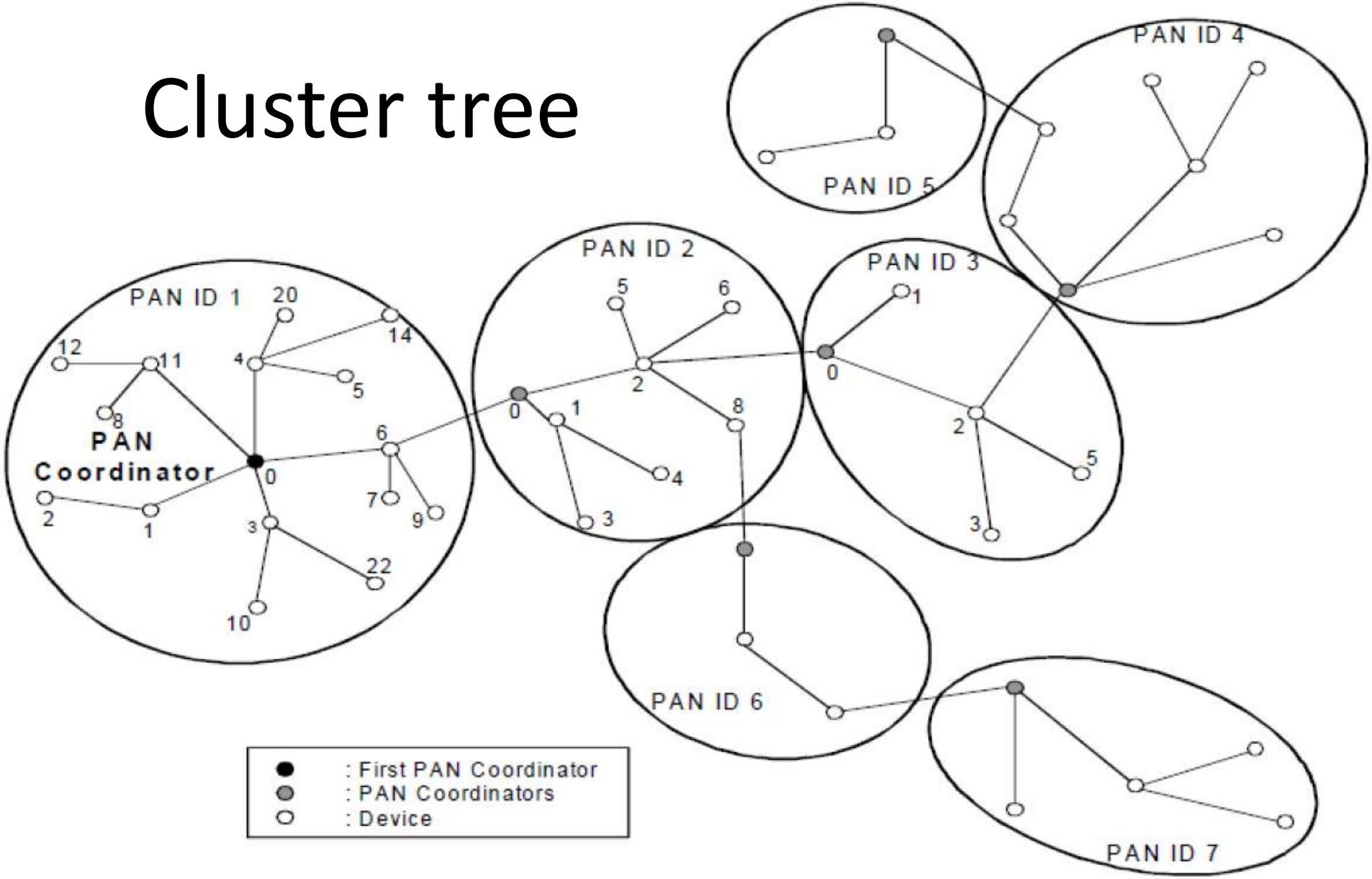
Topológia – hviezda



Topológia – Peer-to-peer



Cluster tree



Max. 255 klastrov po 254 zar. = 64 770 prvkov

Prístup k médiu

CSMA-CA

(Carrier sense multiple access with collision avoidance)

- náhodne dlhé čakanie pred kontrolu média
- lepšie než CSMA-CD

ALOHA

- obsadenosť kanála sa nekontroluje

Hodnotenie voľnosti kanála (Clear Channel Assessment)

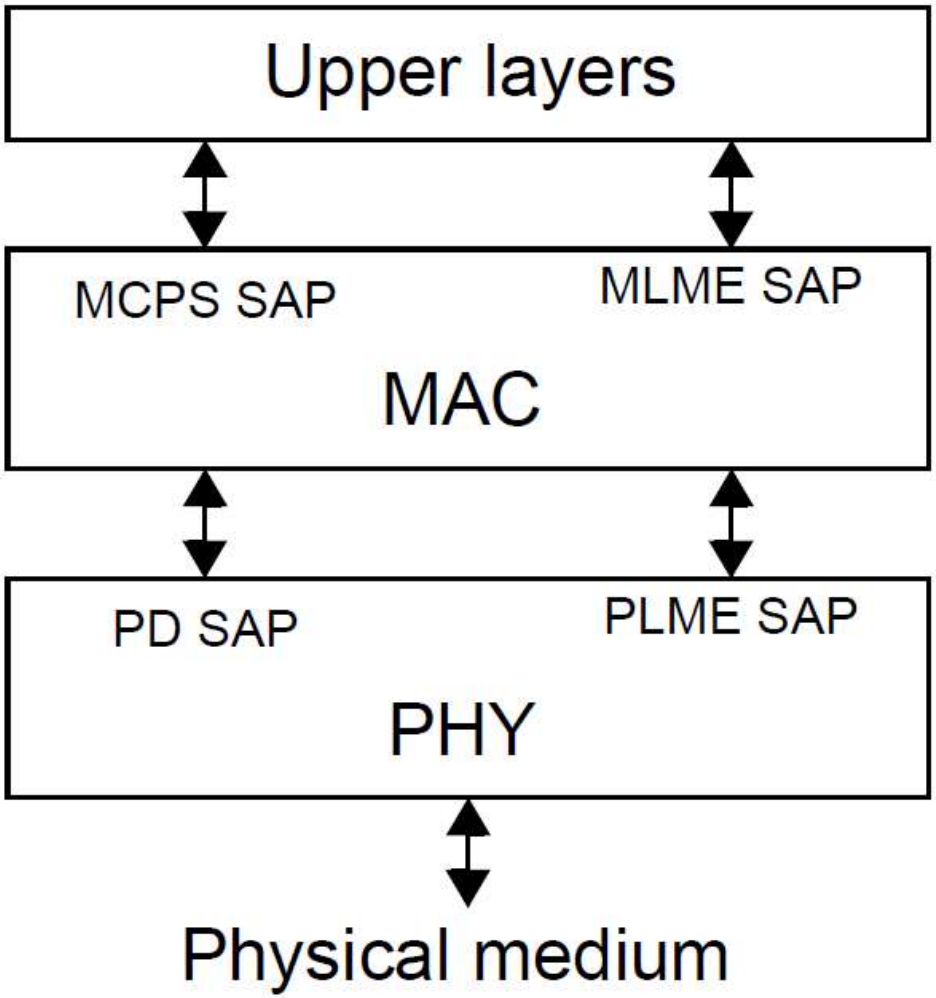
- Energy Detection (ED)
- Carrier Sense
- Carrier Sense + ED
- UWB preamble sense
- ALOHA

Architektúra 802.15.4

- Fyzická vrstva (PHY)
  - RF transceiver
- MAC podvrstva
  - poskytuje prístup k fyzickej vrstve

Prepojenie vrstiev pomocou rozhraní – SAP (Service Access Point)

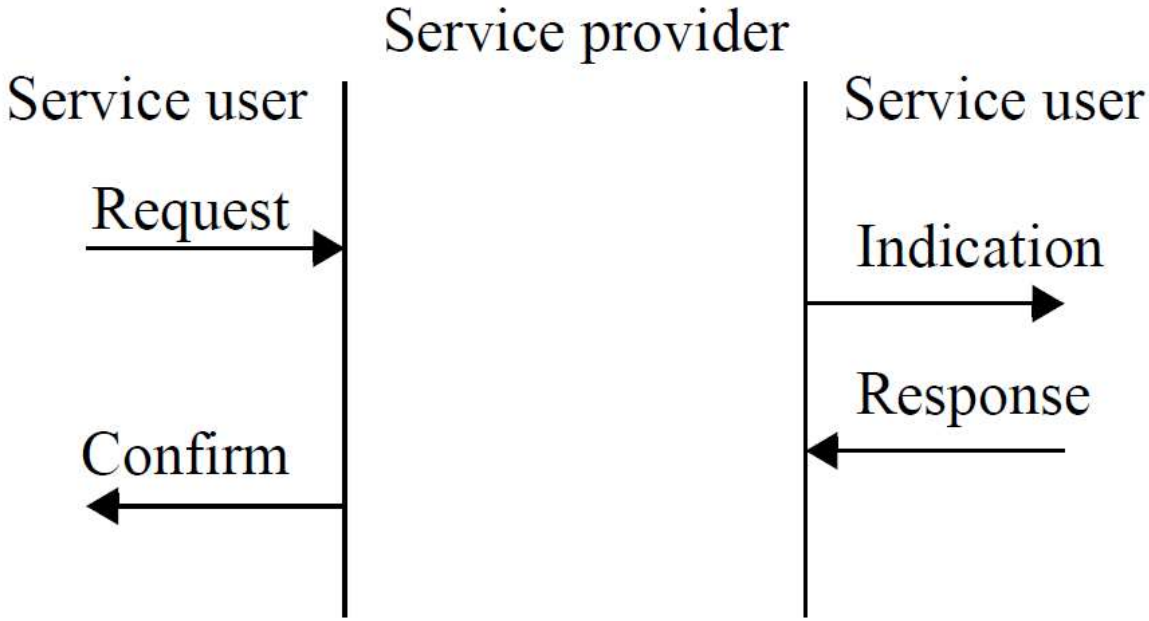
Architektúra 802.15.4



Komunikácia medzi vrstvami

Primitíva:

- Request
- Confirm
- Indication
- Response



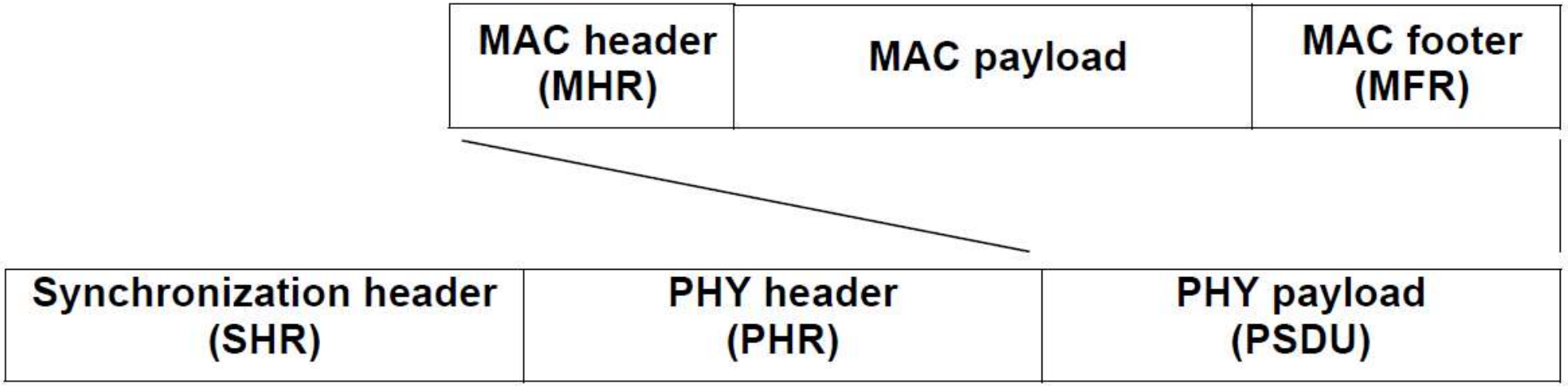
Fyzická vrstva

- Dátové služby
  - prenos paketov (PPDU) cez fyzický kanál
- Služby manažmentu
  - aktivácia/deaktivácia RF
  - výber kanála
  - meranie ED a LQI
  - Clear Channel Assessment
  - Precision ranging (len UWB PHY)

MAC podvrstva

- Dátové služby
  - prenos MPDU (MAC Protocol Data Unit)
- Služby manažmentu
  - prístup ku kanálu
  - manažment beaconov, GTS manažment
  - validácia a potvrdzovanie rámcov,
  - pripojenie a odpojenie zariadení
  - zabezpečenie rámcov

PHY a MAC rámec



MAC rámec

<table>
<tr><th>Octets: 2</th><th>1</th><th>0/2</th><th>0/2/8</th><th>0/2</th><th>0/2/8</th><th>0/5/6/10/14</th><th>variable</th><th>2</th></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td>Destination PAN Identifier</td><td>Destination Address</td><td>Source PAN Identifier</td><td>Source Address</td><td rowspan="2">Auxiliary Security Header</td><td rowspan="2">Frame Payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Addressing fields</td></tr>
<tr><td colspan="7">MHR</td><td>MAC Payload</td><td>MFR</td></tr>
</table>

Frame Control field

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Typy sietí

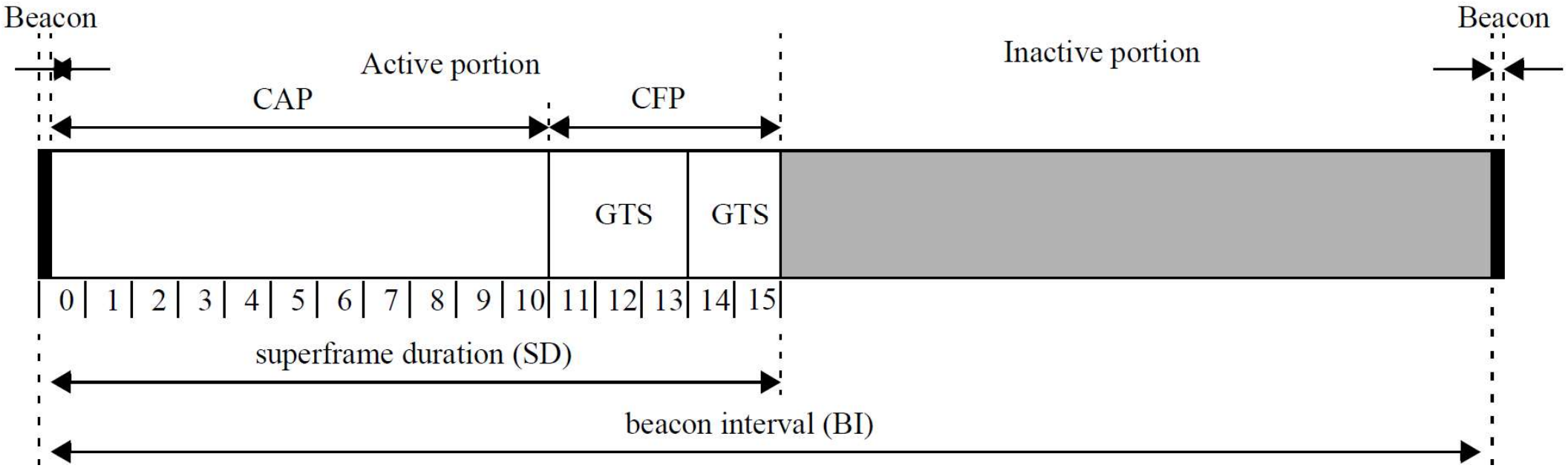
Beacon-enabled PAN

- pravidelné vysielanie beaconov koordinátorom
- synchronizácia zariadení
- čiastočne riadená komunikácia
- „uspávanie“ zariadení
- podpora „low-latency“ zariadení

Nonbeacon-enabled PAN

- „klasické“ siete

Beacony a superrámec



$BI = Base \times 2^{BeaconOrder}$

$SD = Base \times 2^{SuperframeOrder}$

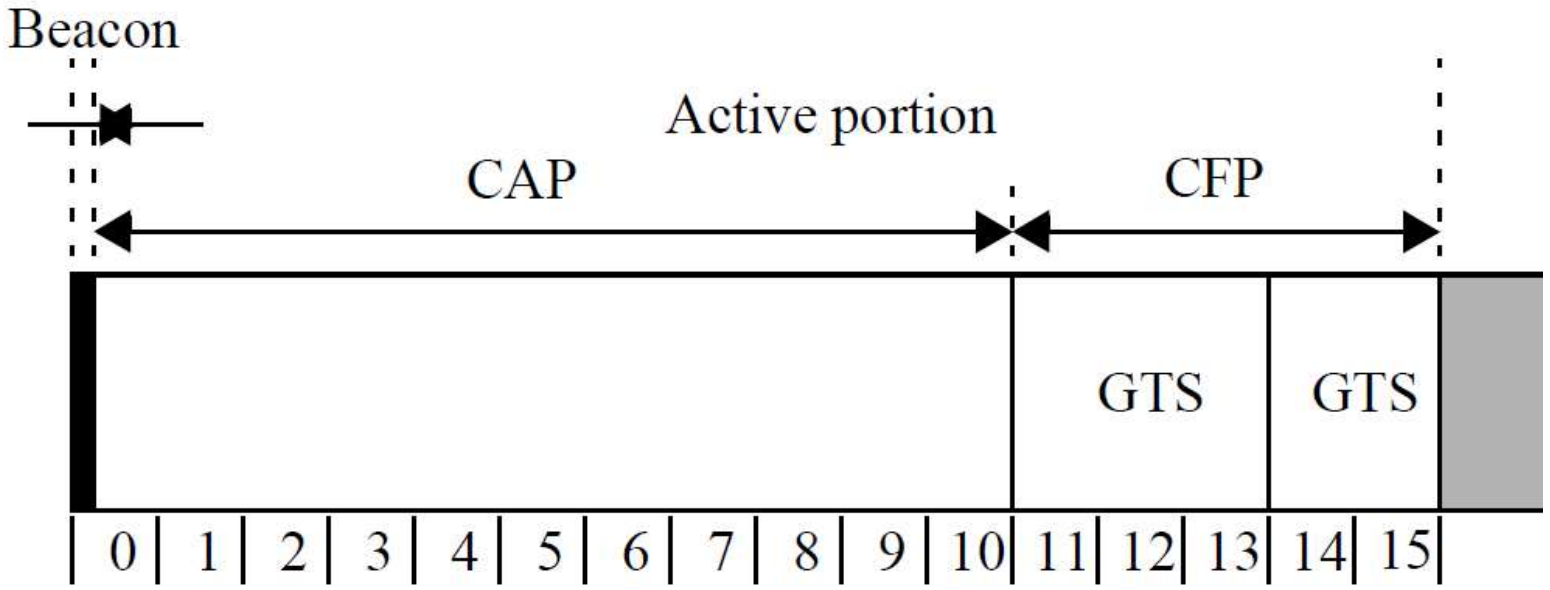
250 kb/s: 15 ms - 251 s

40 kb/s: 24 ms - 393 s

20 kb/s: 48 ms - 786 s

(0 <= SuperframeOrder <= BeaconOrder <= 14)

Štruktúra superrámca



CAP – Contention Access Period

CFP – Contention Free Period

GTS – Guaranteed Time Slot

Beacon

- Beacon order, superframe order
- Veľkosť CAP
- GTS
- Povolenie asociácie
- PAN kordinátor
- Indikácia čakajúcich paketov

Typy prenosov

- Zariadenie -> zariadenie
  (peer-to-peer)
- Zariadenie -> koordinátor
  (hviezda, peer-to-peer)
- Koordinátor -> zariadenie
  (hviezda, peer-to-peer)

Typy prenosov

Zariadenie -> zariadenie

- Nutná synchronizácia

Zariadenie -> koordinátor

- Beacon enabled PAN
  - synchronizácia so superrámcom
- Non-beacon PAN

Koordinátor -> zariadenie

Nepriamy prenos

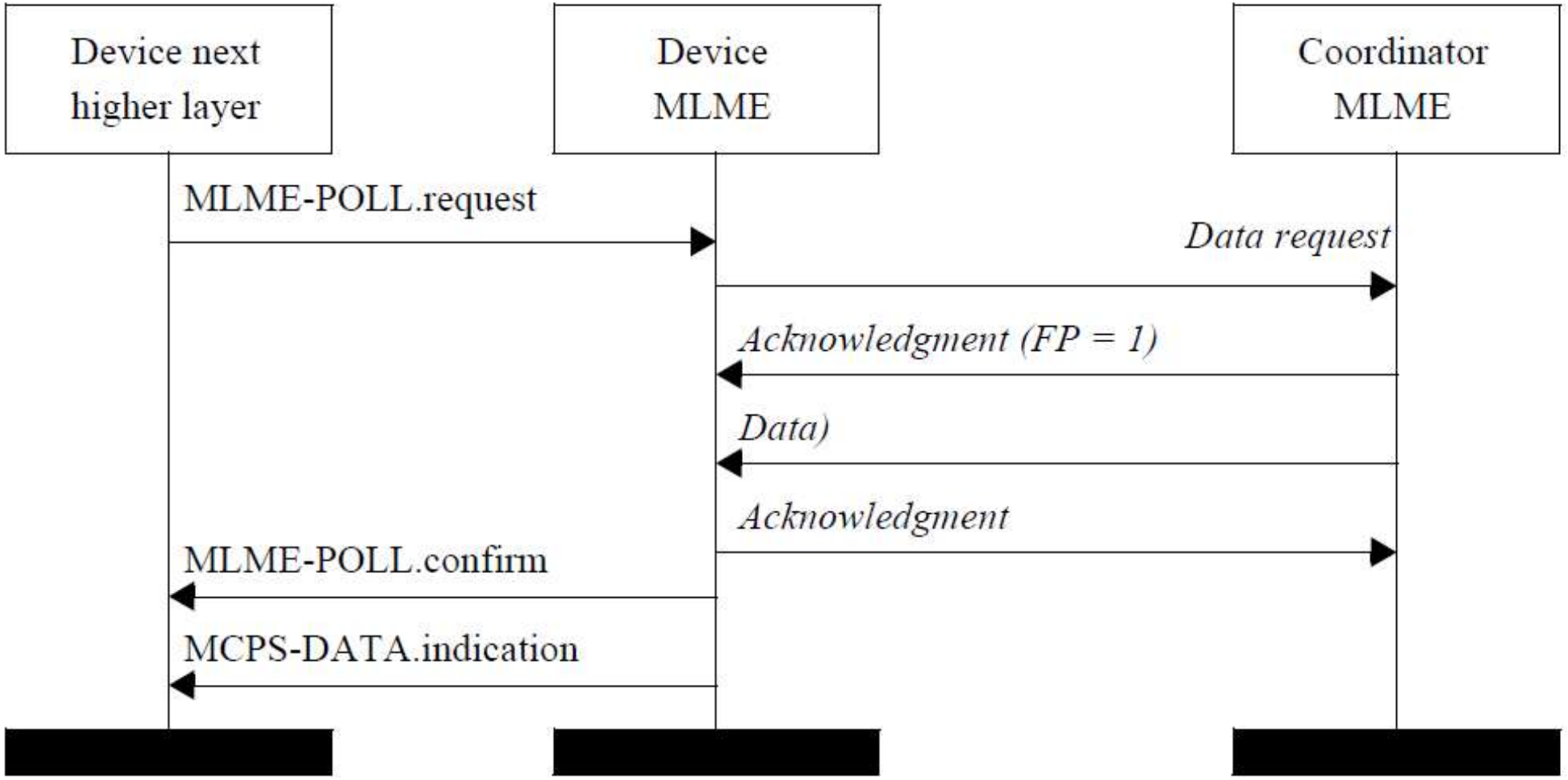
Beacon enabled PAN

- Indikácia správy v beacone
- Vyžiadanie a prenos správy počas CAP

Non-beacon PAN

- Prenos na výzvu (polling)

Polling


Device next higher layer
Device MLME
Coordinator MLME
MLME-POLL.request
Data request
Acknowledgment (FP = 1)
Data)
Acknowledgment
MLME-POLL.confirm
MCPS-DATA.indication

Spoľahlivosť prenosu

- Potvrdzovanie (ACK rámec)
- Opakovaný prenos

Nepotvrdzuje sa

- Beacon
- ACK rámec
- Broadcast

Zabezpečenie komunikácie

- Obmedzenia dané vlastnosťami siete
- Symetrické šifrovanie (AES 128)

Hlavné bezpečnostné služby

- data confidentality
- data authenticity
- replay protection

Úrovne zabezpečenia

- 0 – žiadne
- 1-3 – autenticita (MIC-32, MIC-64, MIC-128)
- 4 – šifrovanie
- 5-7 – autenticita a šifrovanie

Linkové a skupinové kľúče

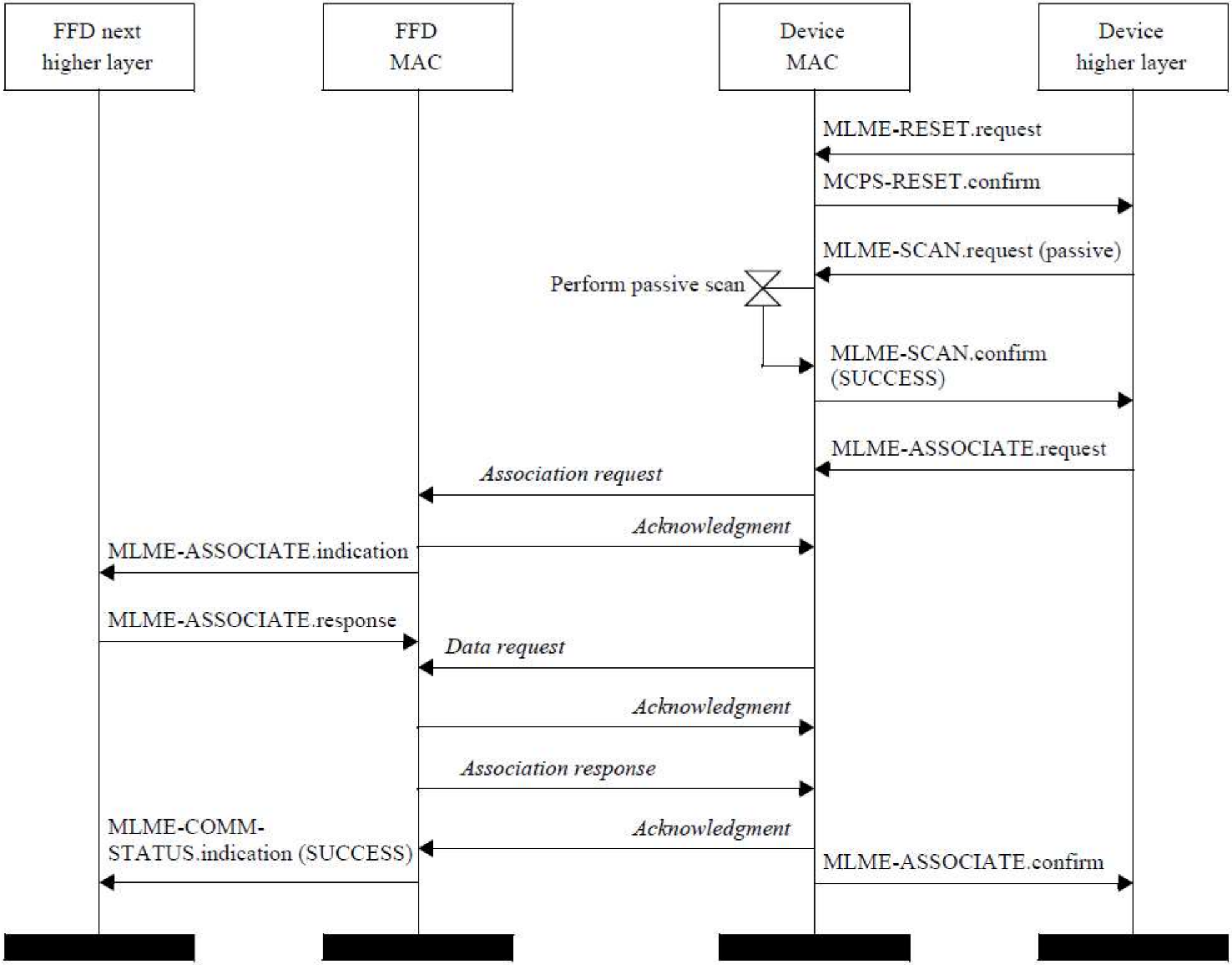
MIC = Message Integrity Code

Vytvorenie siete

- Skenovanie kanálov
- Detekcia energie
- Výber kanála
- Výber PAN ID
- (Štart vysielania beaconov)

Pripojenie (asociácia)

- Skenovanie kanálov
- Výber siete
- Žiadosť o pripojenie
- Pridelenie adresy
- Komunikácia


FFD next higher layer
FFD MAC
Device MAC
Device higher layer
MLME-RESET.request
MCPS-RESET.confirm
MLME-SCAN.request (passive)
Perform passive scan
MLME-SCAN.confirm (SUCCESS)
MLME-ASSOCIATE.request
Association request
Acknowledgment
MLME-ASSOCIATE.indication
MLME-ASSOCIATE.response
Data request
Acknowledgment
Association response
Acknowledgment
MLME-COMM-STATUS.indication (SUCCESS)
MLME-ASSOCIATE.confirm

Odpojenie a osirenie

- Odpojenie zariadenia
  - Disassociation Notification príkaz
- Osirenie zariadenia
  - Orphan scan a Realignment
  - nové pripojenie

Vytvorené v rámci projektu KEGA 026TUKE-4/2021