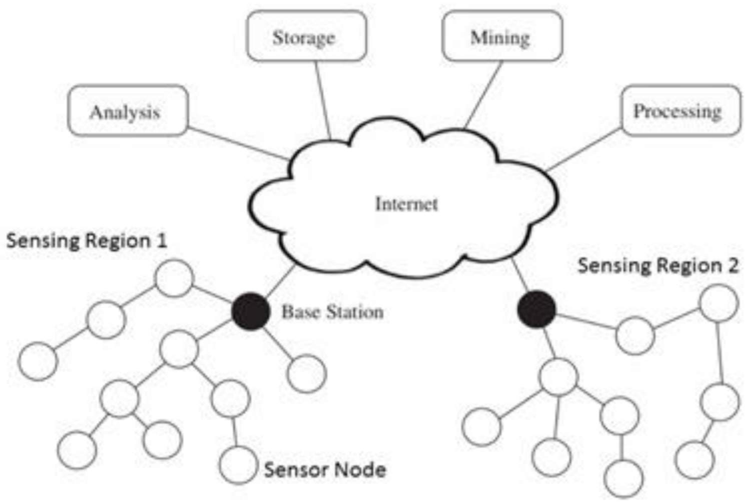
CS 439: Wireless Networking

IEEE 802.15.4/ZigBee

 Fall 2020

IEEE 802.15.4

- Designed for wireless sensor networks
  - Interest increased in the early 2000s
  - Used in Low Data applications
  - Needed to be Cost Effective
  - Battery reliant



IEEE 802.15.4: Motivation

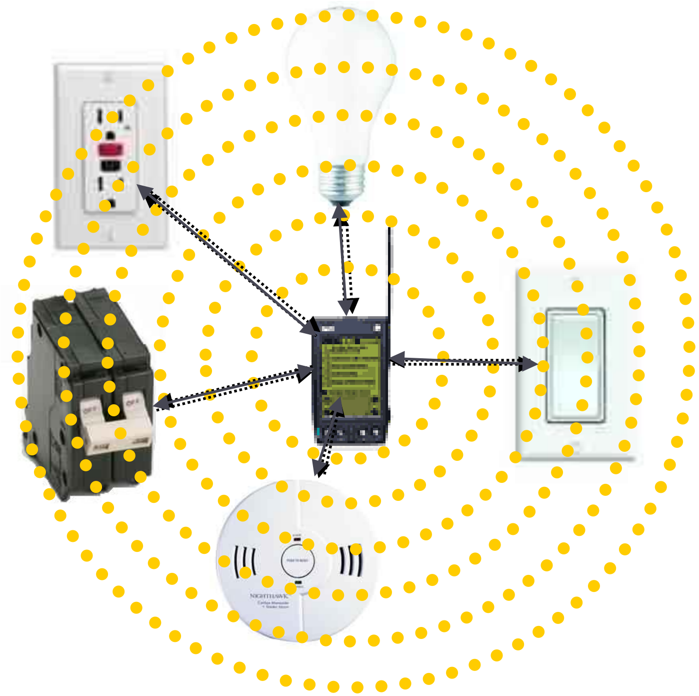
- WiFi was too heavyweight
- Bluetooth was complex
- Bluetooth was proprietary at the time

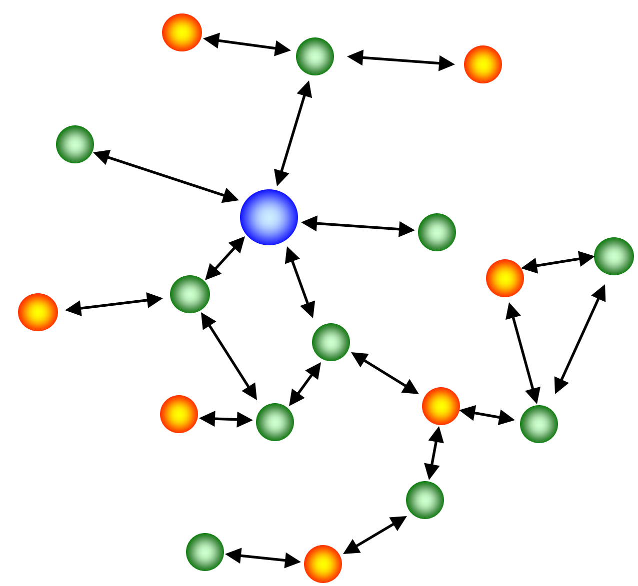
Zigbee and 802.15.4

- IEEE 802.15.4
  - Released in 2003
  - Defines MAC and PHY layer
  - Basis for ZigBee
  - Low Data Rate, Low Power
- ZigBee
  - Released in 2005
  - Defines Network Layer and above

802.15.4 Applications Space

- Home Networking
- Automotive Networks
- Industrial Networks
- Interactive Toys
- Remote Metering

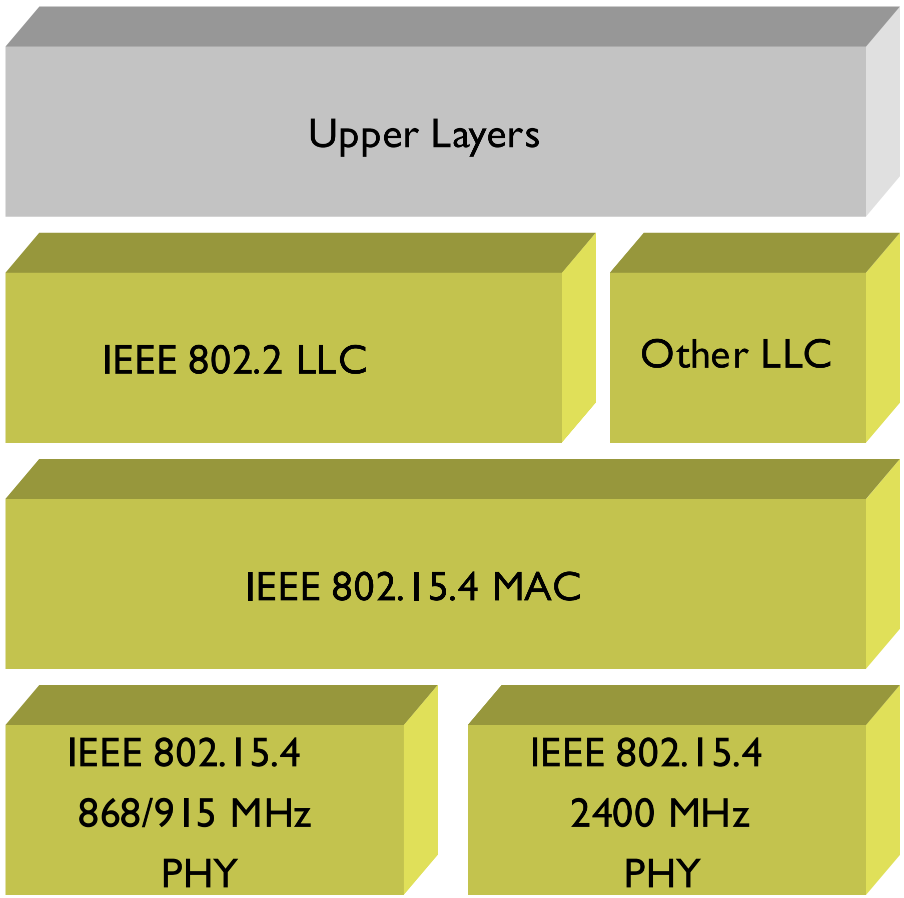




802.15.4 General Characteristics

- Frequency Bands
  - 16 channels in the 2.4GHz ISM band
  - 10 channels in the 915MHz ISM band
  - 1 channel in the European 868MHz band.
- Data rates
  - 250 kb/s, 40 kb/s and 20 kb/s.
- Star or Peer-to-Peer operation
- Support for low latency devices
- CSMA-CA channel access
- Dynamic device addressing
- Fully handshaked protocol for transfer reliability
- Low power consumption

802.15.4 Architecture



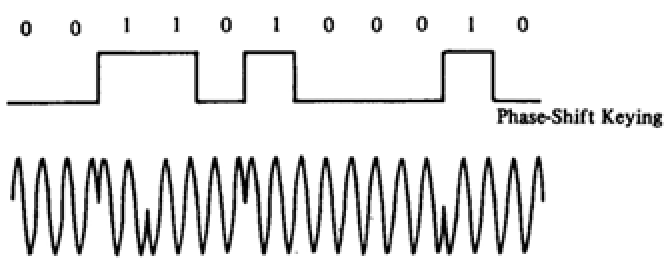
- **Packet generation**
- **Packet reception**
- **Data transparency**
- **Power Management**

802.15.4 Physical Layers

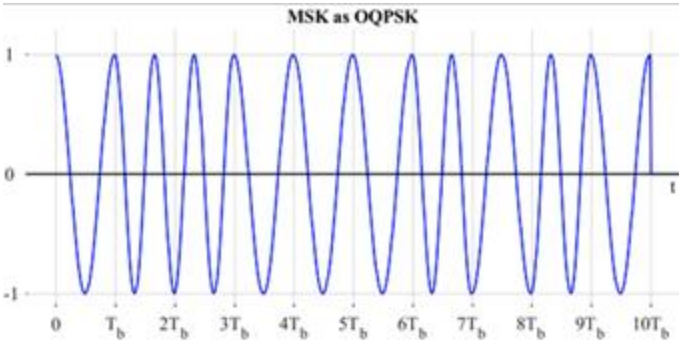
PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

802.15.4 Physical Layers

- O-QPSK modulation
  - Offset Quadrature Phase-Shift Keying
  - Twice the data rate of BPSK for same BER
  - Cost: most complicated design of receivers
  - 4 bits per symbol
- 802.15.4 bit rate at 2.4 GHz: 2000 chips/s = 250 kbps = 62.5 kBaud

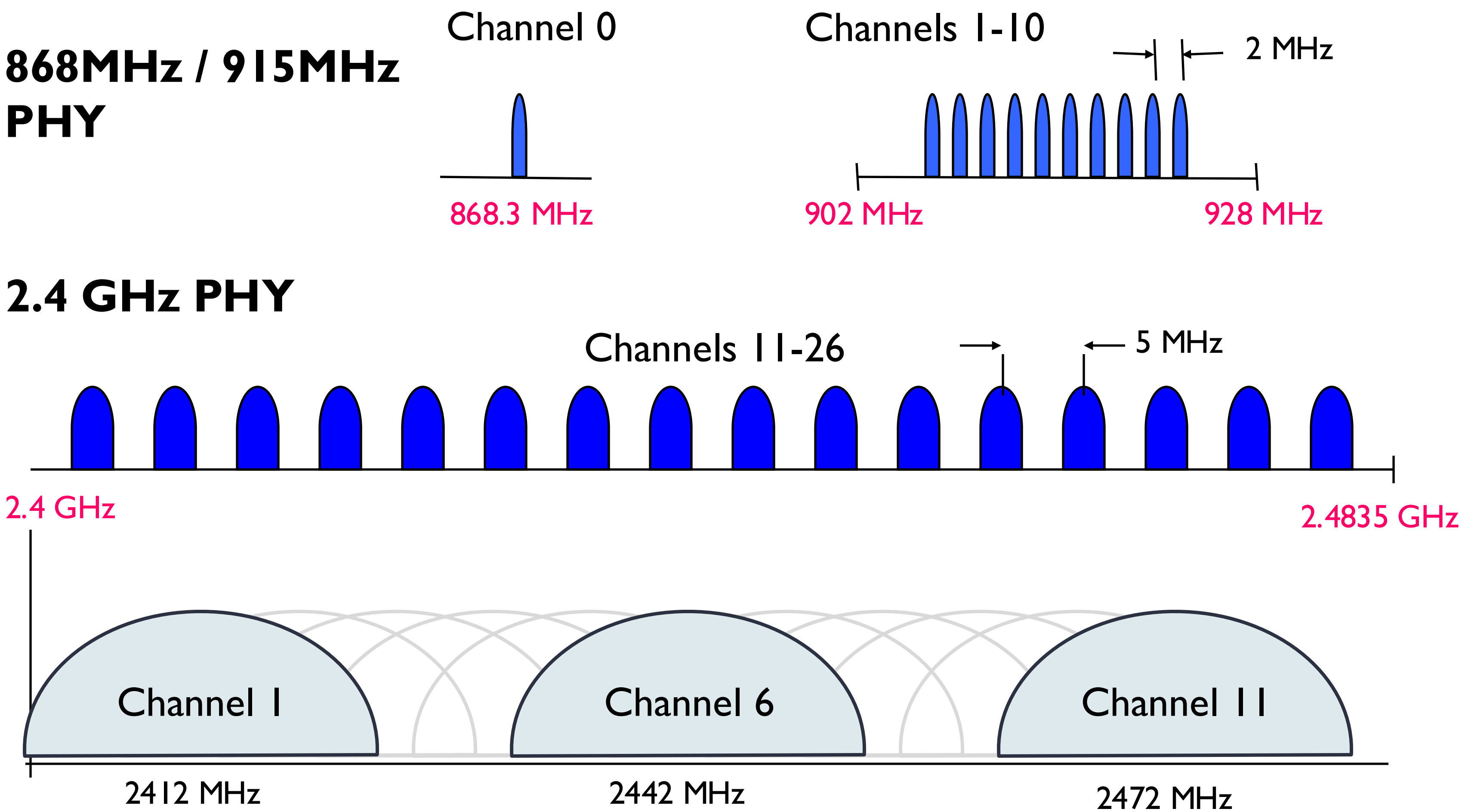


Standard BPSK



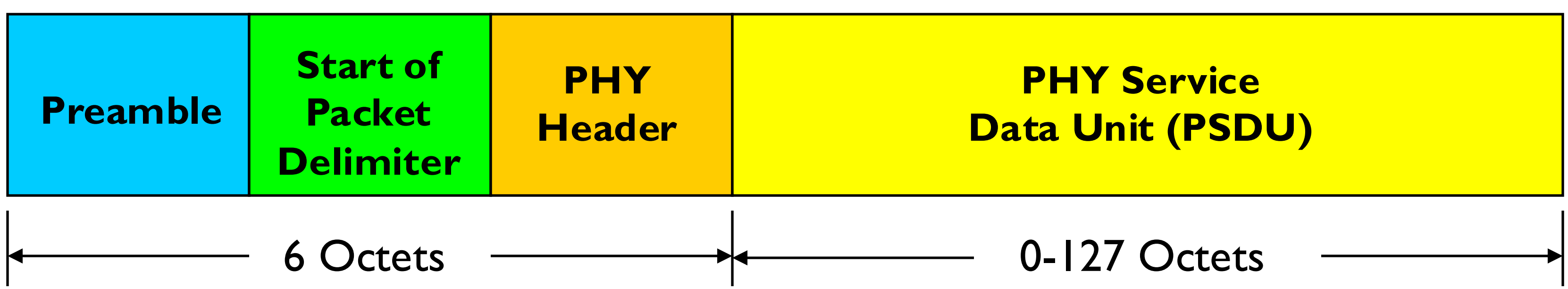
O-QPSK

IEEE 802.15.4 PHY: Frequency Bands



IEEE 802.15.4 PHY: Packet Structure

- PHY Packet Fields
  - Preamble (32 bits) – synchronization
  - Start of Packet Delimiter (8 bits)
  - PHY Header (8 bits) – PSDU length
  - PSDU (0 to 1016 bits) – Data field

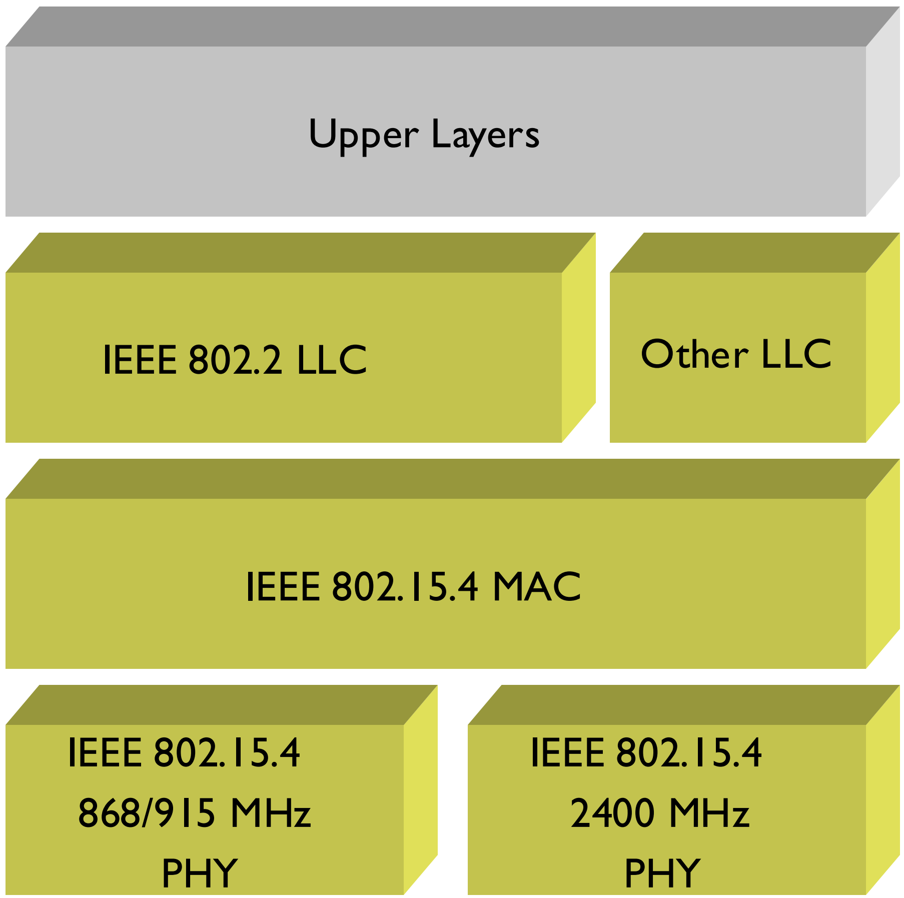


IEEE 802.15.4 PHY: Modulation/Spreading

- 2.4 GHz PHY
  - 250 kb/s (4 bits/symbol, 62.5 kBaud)
  - Data modulation is 16-ary orthogonal modulation
  - 16 symbols are ~orthogonal set of 32-chip PN codes
  - Chip modulation is MSK at 2.0 Mchips/s

- 868MHz/915MHz PHY
  - Symbol Rate
    - 868 MHz Band: 20 kb/s (1 bit/symbol, 20 kBaud)
    - 915 MHz Band: 40 kb/s (1 bit/symbol, 40 kBaud)
  - Data modulation is BPSK with differential encoding
  - Spreading code is a 15-chip m-sequence
  - Chip modulation is BPSK at
    - 868 MHz Band: 300 kchips/s
    - 915 MHz Band: 600 kchips/s

802.15.4 Architecture



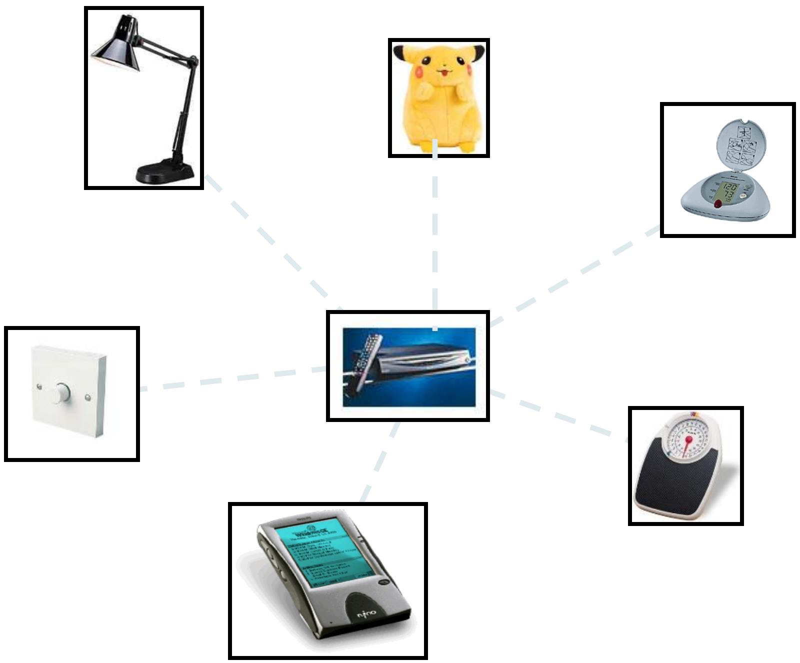
- Channel acquisition
- Contention mgt
- NIC address
- Error Correction

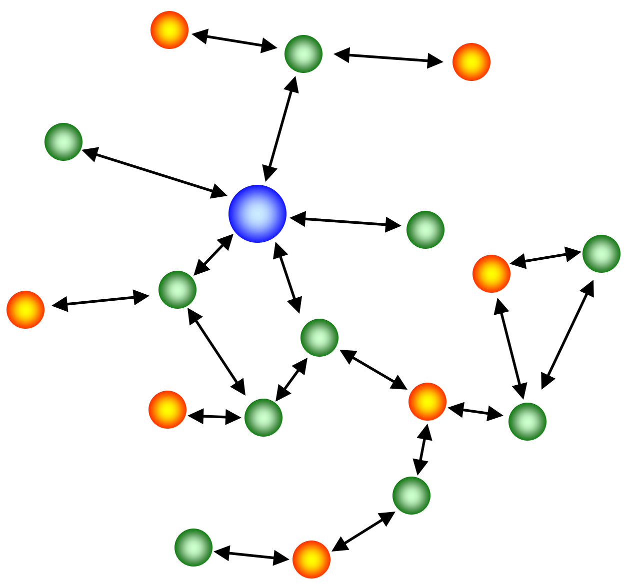
IEEE 802.15.4 MAC: Design Drivers

- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

Simple but flexible protocol

IEEE 802.15.4 MAC: Network Topologies

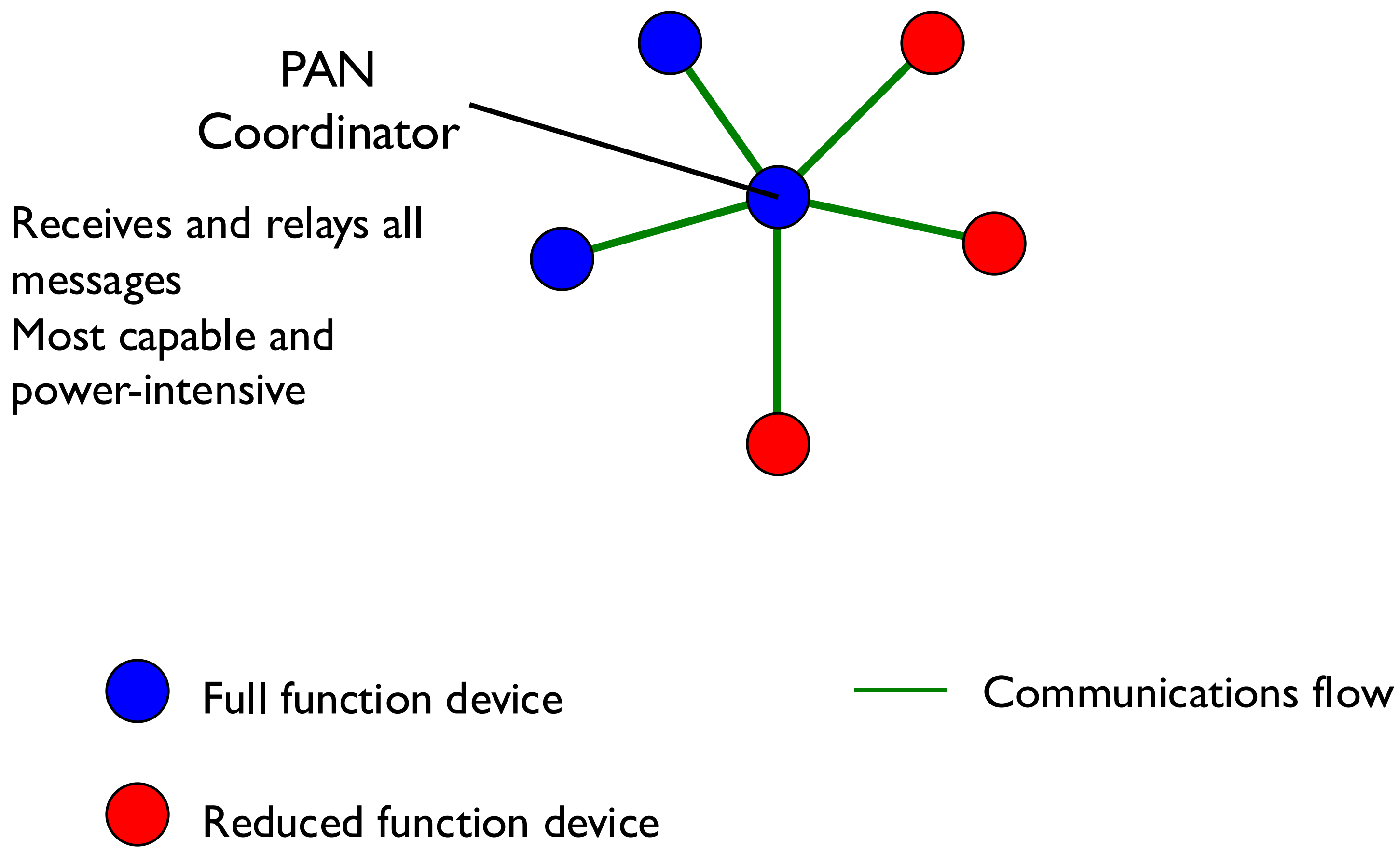




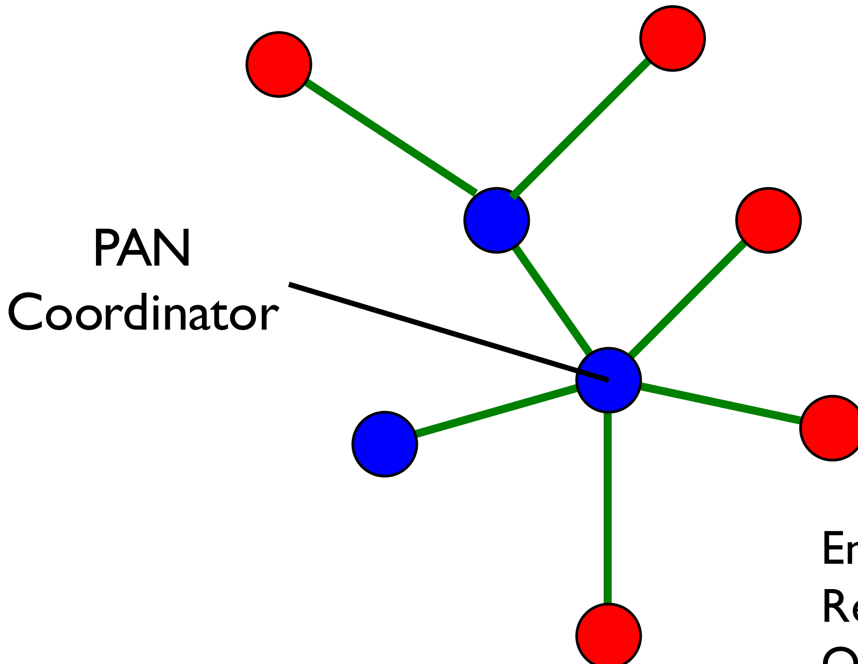
IEEE 802.15.4 MAC: Device Classes

- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

IEEE 802.15.4 MAC: Star Topology



IEEE 802.15.4 MAC: Tree Topology



Coordinators (a.k.a. Routers)
Full function device
Control “clusters”
Receives and relays to its children
Communicates up to parent coordinator

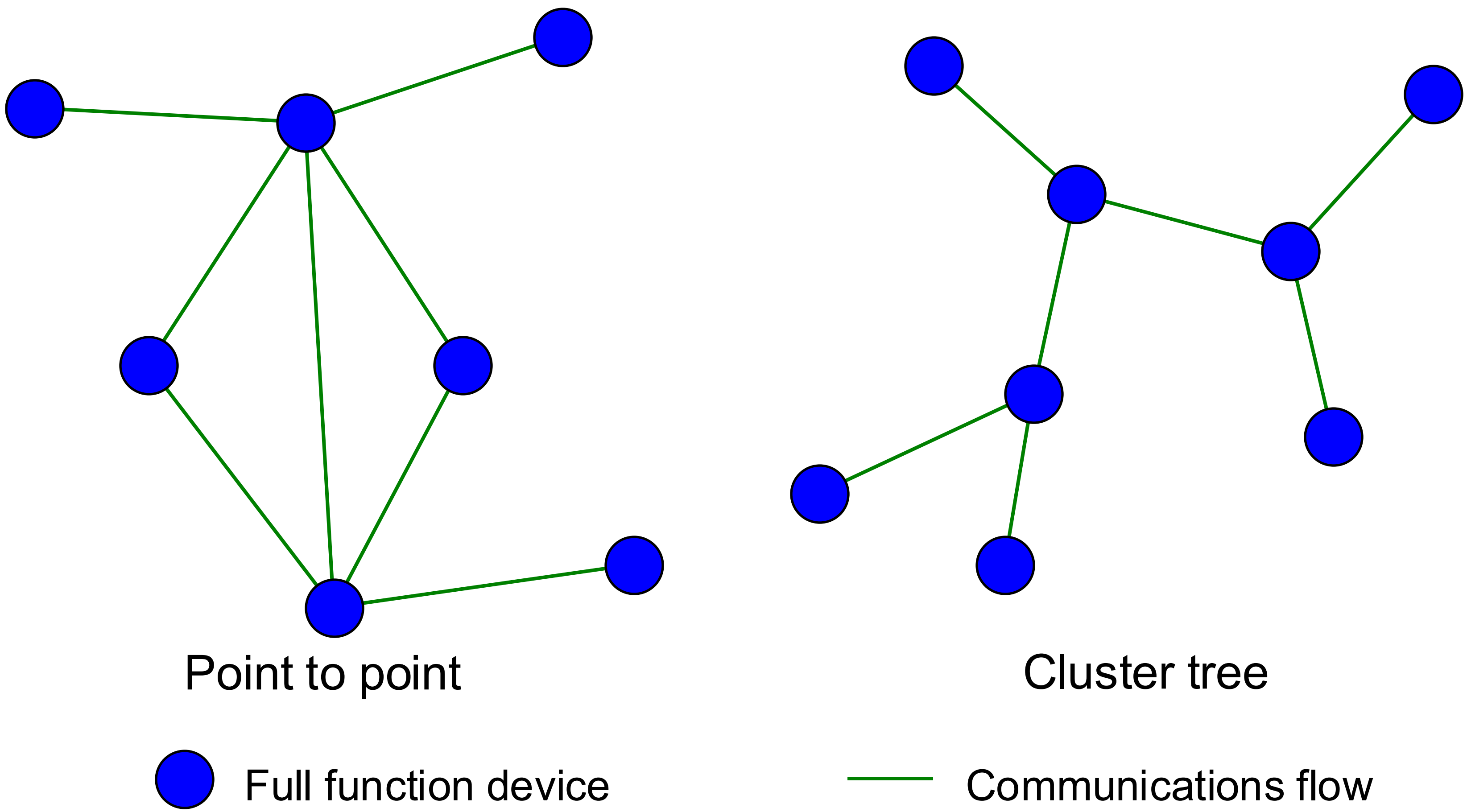
End Devices
Reduced function device
Only communicate with single parent coordinator
Least capable and power intensive

Full function device

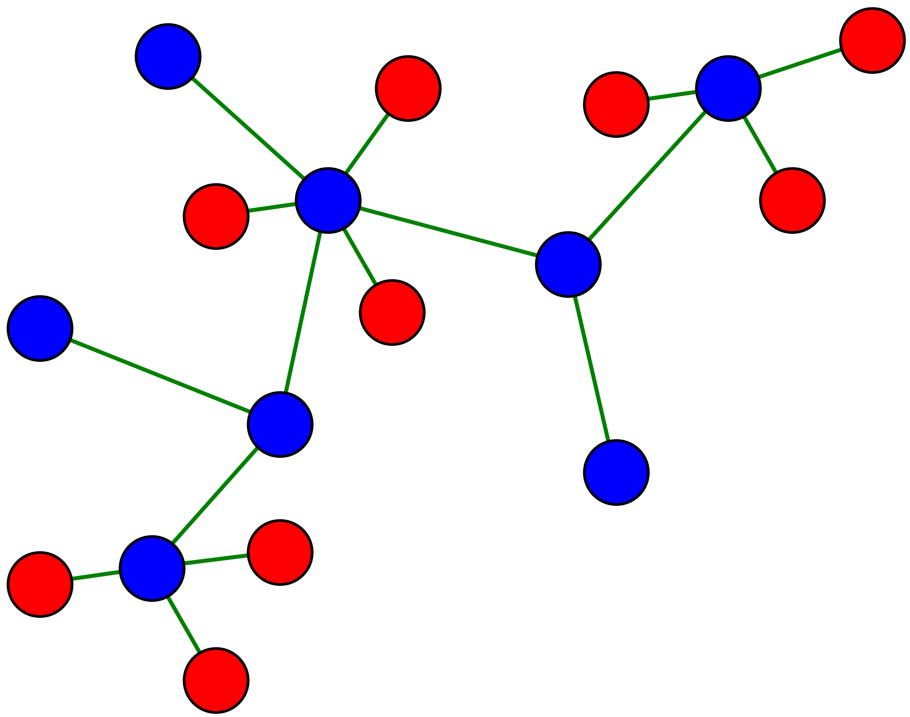
Reduced function device

Communications flow

IEEE 802.15.4 MAC: Peer-Peer Topology



IEEE 802.15.4 MAC: Combined Topology



Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

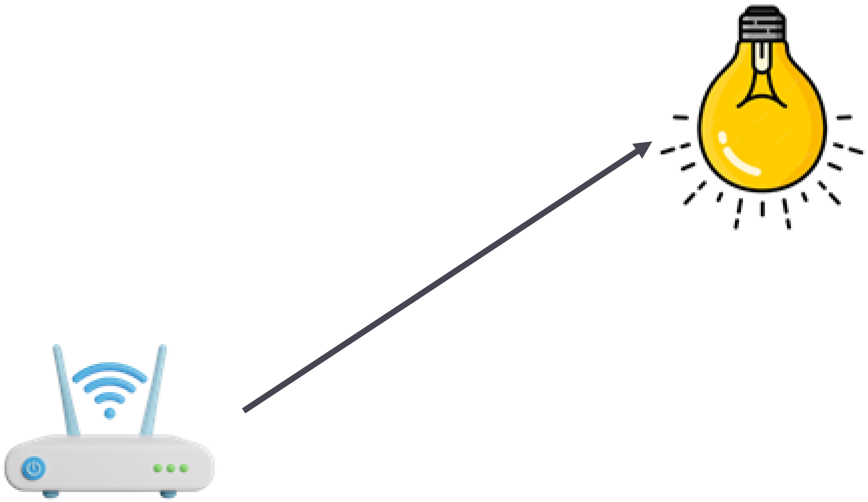
Full function device

Reduced function device

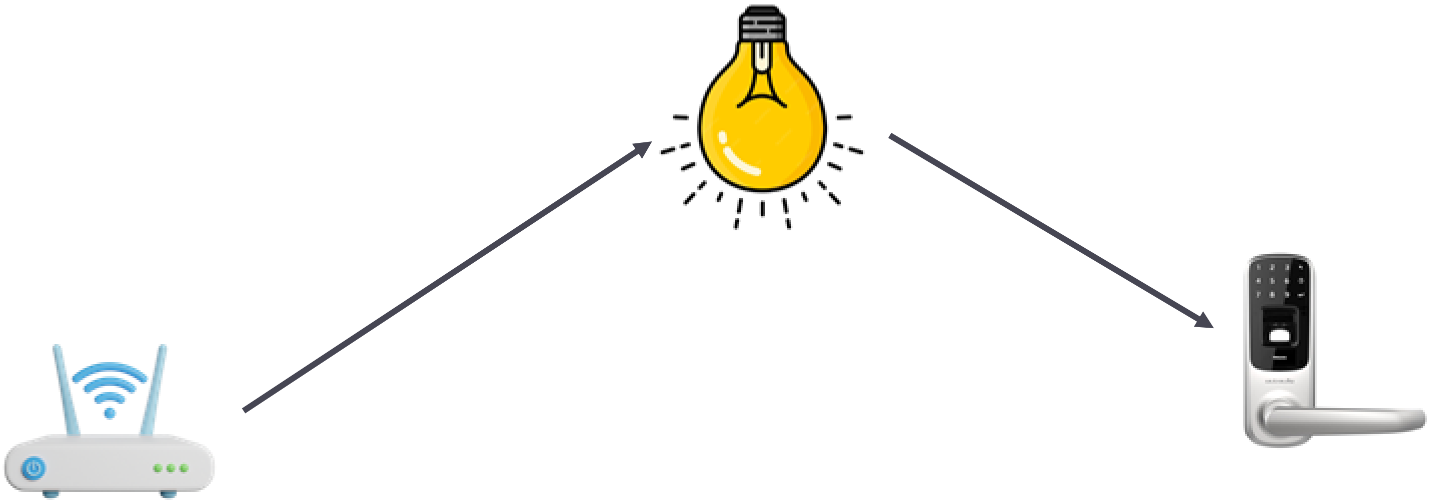
Communications flow

Network Example

Network Example



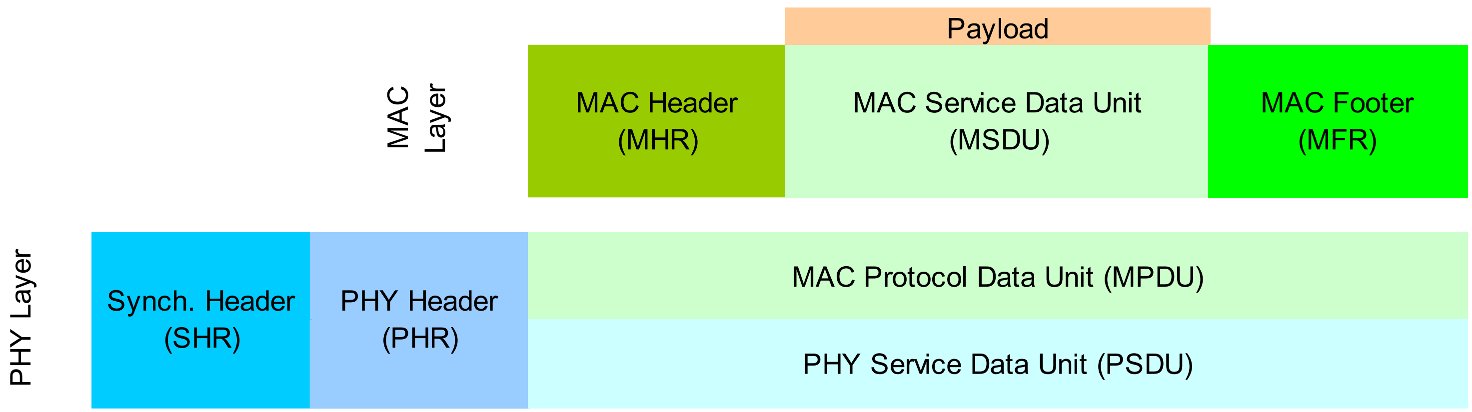
Network Example



IEEE 802.15.4 MAC: Addressing

- All devices have IEEE addresses
- Short addresses can be allocated
- Addressing modes:
  - Network + device identifier (star)
  - Source/destination identifier (peer-peer)

IEEE 802.15.4 MAC: General Frame Structure

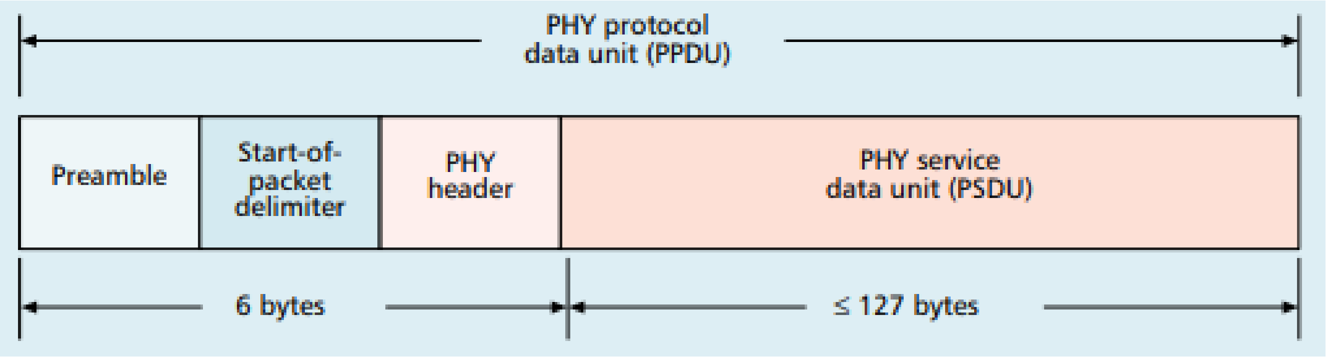


4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

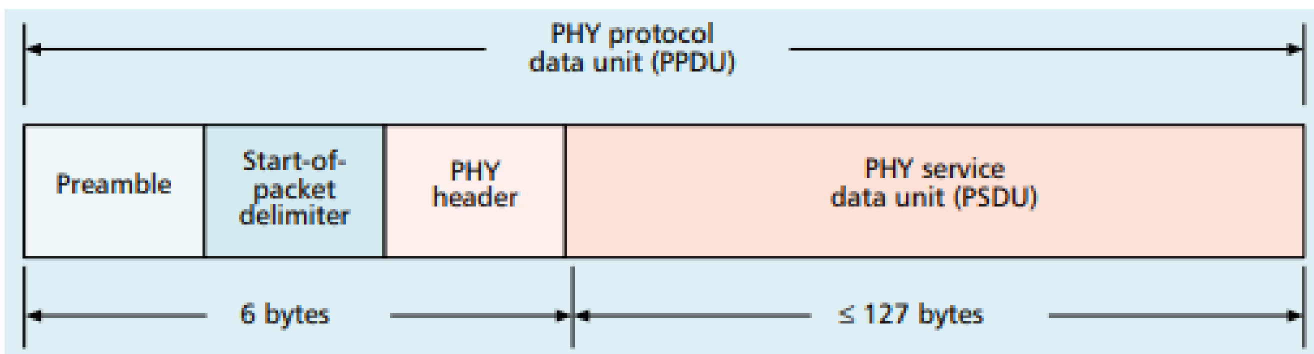
Base packet format

- Synchronization
  - Preamble: four bytes of zeros
  - Start-of-Packet: 0xA7
- PHY Header
  - One field: length 0-127
  - Why still 8 bits?



Base packet format

- Synchronization
  - Preamble: four bytes of zeros
  - Start-of-Packet: 0xA7
- PHY Header
  - One field: length 0-127
  - Why still 8 bits?   Because computers depend on bytes



IEEE 802.15.4 MAC: General Frame Structure

Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						MAC payload	MAC footer

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Sequrity enabled	Frame pending	Ack. Req.	Intra PAN	Reserved	Dest. addressing mode	Reserved	Source addressing mode

Frame control field

IEEE 802.15.4 MAC: Beacon Frame Structure

Octets:2	1	4 or 10	2	variable	variable	variable	2
Frame control	Beacon sequence number	Source address information	Superframe specification	GTS fields	Pending address fields	Beacon payload	Frame check sequence
MAC header			**MAC payload**				**MAC footer**

Bits: 0-3	4-7	8-11	12	13	14	15
Beacon order	Superframe order	Final CAP slot	Battery life extension	Reserved	PAN coordinator	Association permit

- Sent periodically at start of Superframes (if in use)
- Sent without CSMA/CA
- Source address only, broadcast to everyone
- Superframe details, including Guaranteed Time Slots (if any)
- Pending addresses lists devices for which Coordinator has data

IEEE 802.15.4 MAC: Command Frame Structure

Octets:2	1	4 to 20	1	variable	2
Frame control	Data sequence number	Address information	Command type	Command payload	Frame check sequence
MAC header			**MAC payload**		**MAC footer**

- Command Frame Types
  - Association request
  - Association response
  - Disassociation notification
  - Data request
  - PAN ID conflict notification
  - Orphan Notification
  - Beacon request
  - Coordinator realignment
  - GTS request

IEEE 802.15.4 MAC: Frame Structure

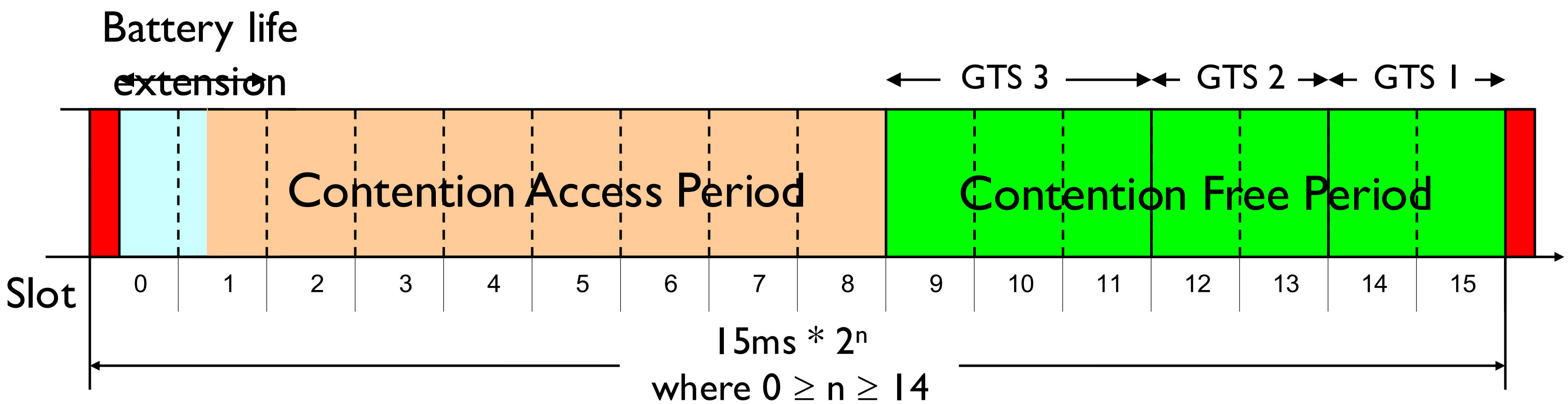
Data Frame Format

Octets:2	1	4 to 20	variable	2
Frame control	Data sequence number	Address information	Data payload	Frame check sequence
MAC header			**MAC Payload**	**MAC footer**

Acknowledgement Frame Format

Octets:2	1	2
Frame control	Data sequence number	Frame check sequence
MAC header		**MAC footer**

IEEE 802.15.4 MAC: Optional Superframe Structure



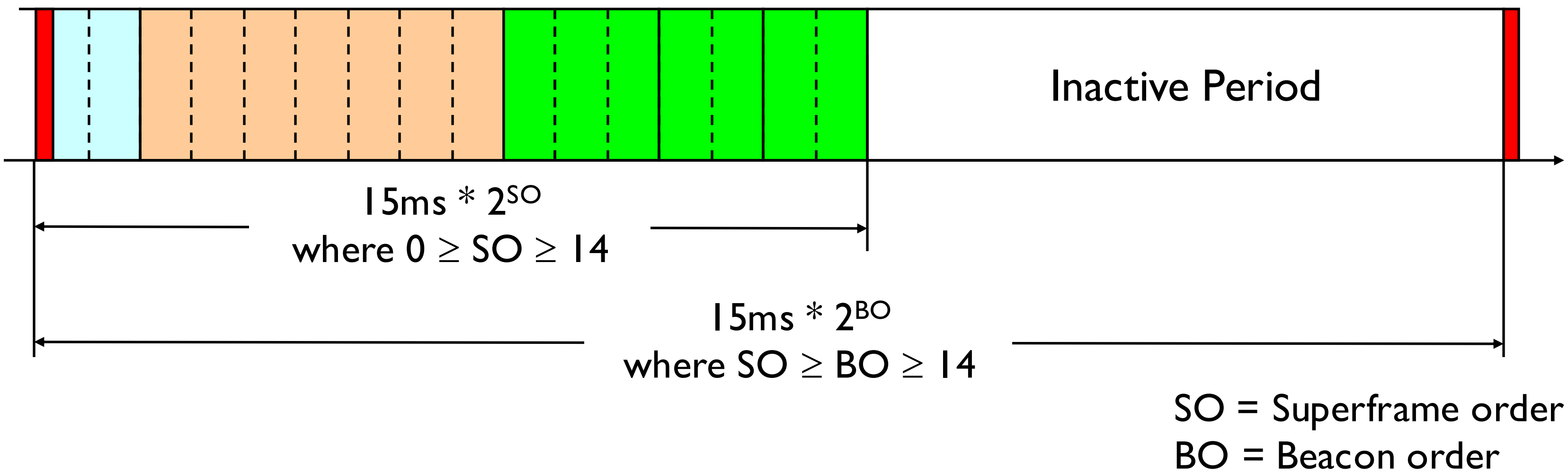
Network beacon — Transmitted by network coordinator. Contains network information, frame structure and notification of pending node messages.

Beacon extension period — Space reserved for beacon growth due to pending node messages

Contention period — Access by any node using CSMA-CA

Guaranteed Time Slot — Reserved for nodes requiring guaranteed bandwidth [n = 0]. No CSMA/CA for CFP

IEEE 802.15.4 MAC: Optional Superframe Structure

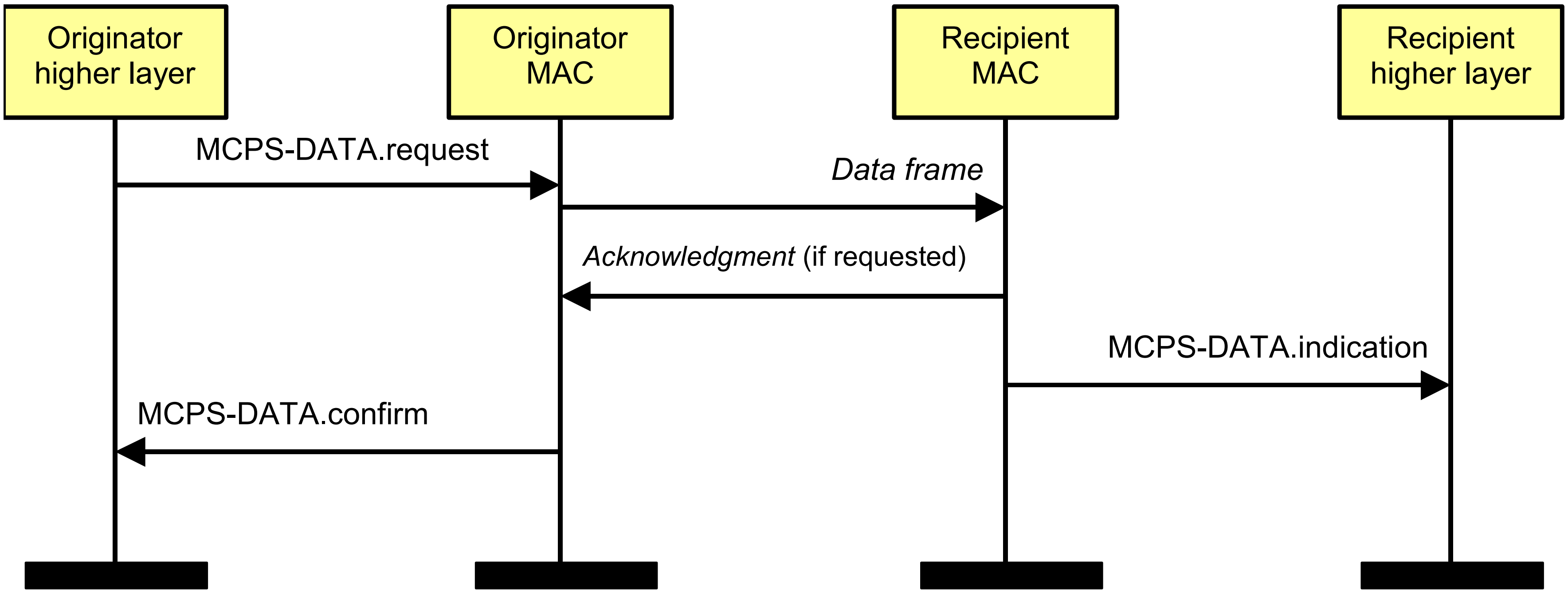


- Superframe may have inactive period

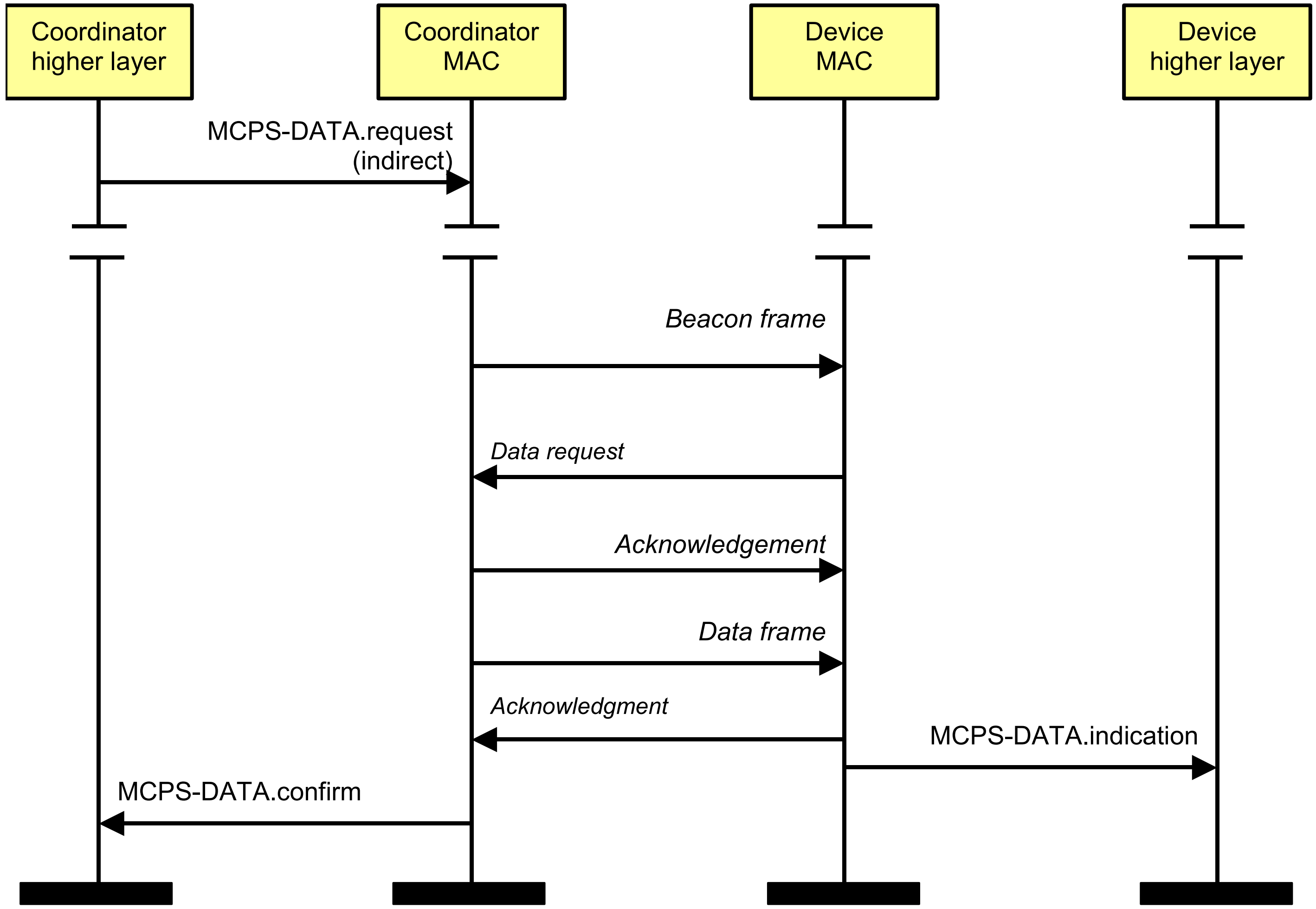
IEEE 802.15.4 MAC: Traffic Types

- Periodic data
  - Application defined rate (e.g. sensors)
- Intermittent data
  - Application/external stimulus defined rate (e.g. light switch)
- Repetitive low latency data
  - Allocation of time slots (e.g. mouse)

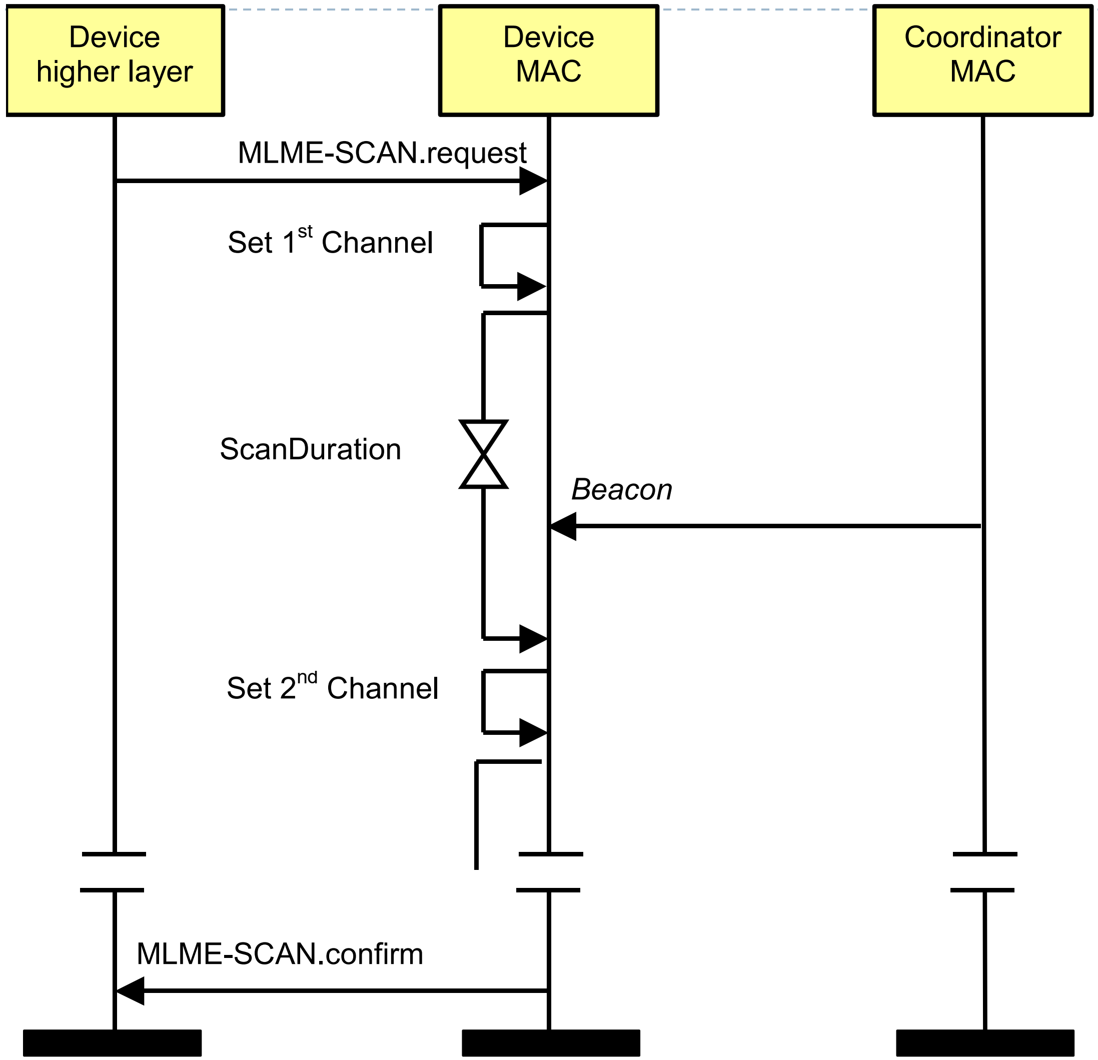
Data Transfer
Message Sequence Diagram



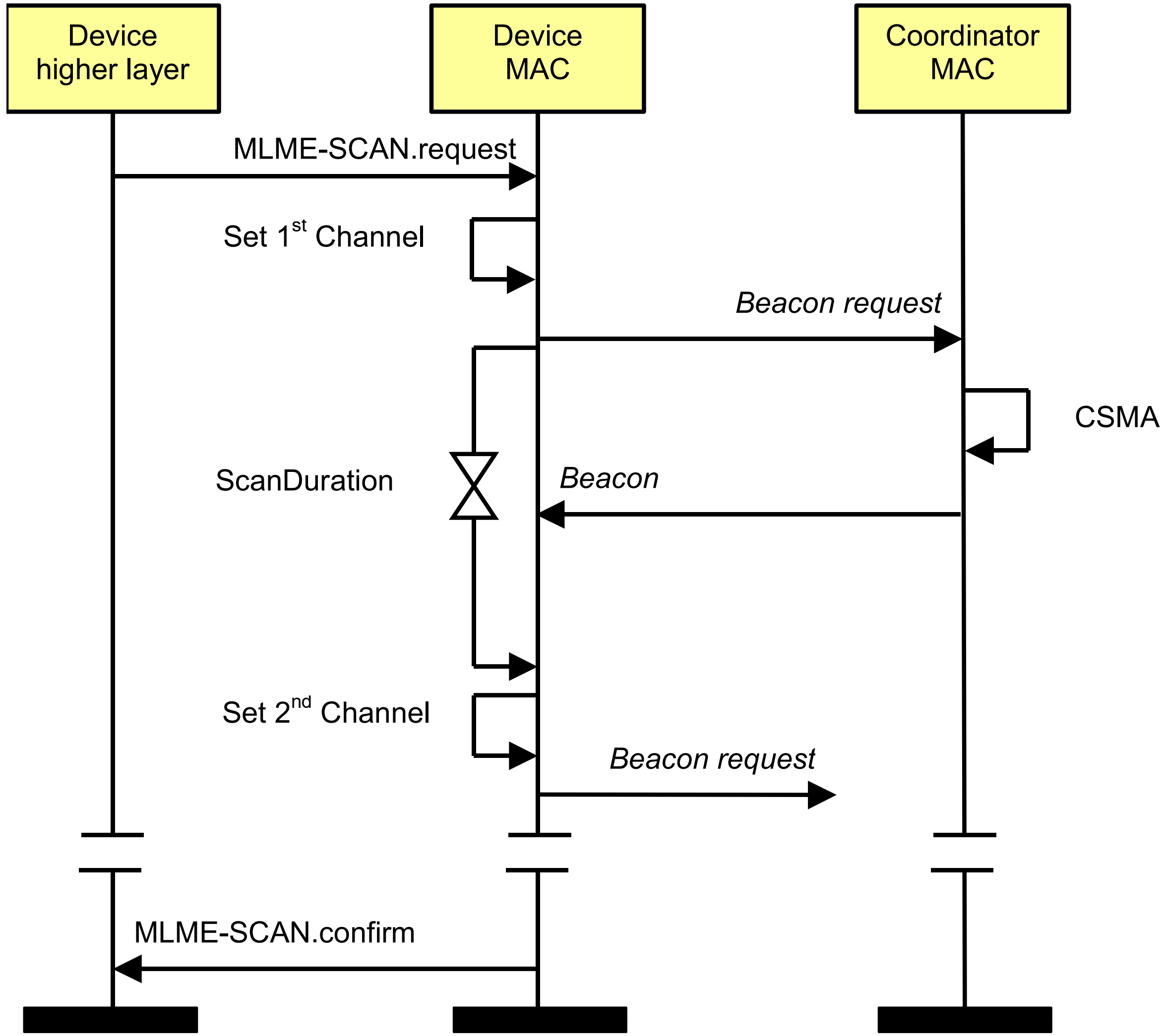
Indirect Data Transfer
Message Sequence Diagram



Passive Scan



Active Scan


Device
higher layer
Device
MAC
Coordinator
MAC
MLME-SCAN.request
Set 1st Channel
Beacon request
CSMA
ScanDuration
Beacon
Set 2nd Channel
Beacon request
MLME-SCAN.confirm

IEEE 802.15.4 MAC: Power

- Major Source of Energy Waste
- Consumption occurs in three domains:
  - Sensing
  - Data processing
  - Communications as the major consumer of energy

- Energy Communication waste
  - Idle listening as dominant factor in most applications
  - Collision
  - Overhearing
  - Control packet overhead

- Main design of energy efficient MAC protocols
  - Reduction or elimination of the energy communication waste in particular idle listening
  - Central approach to reduce idle listening through Duty cycling

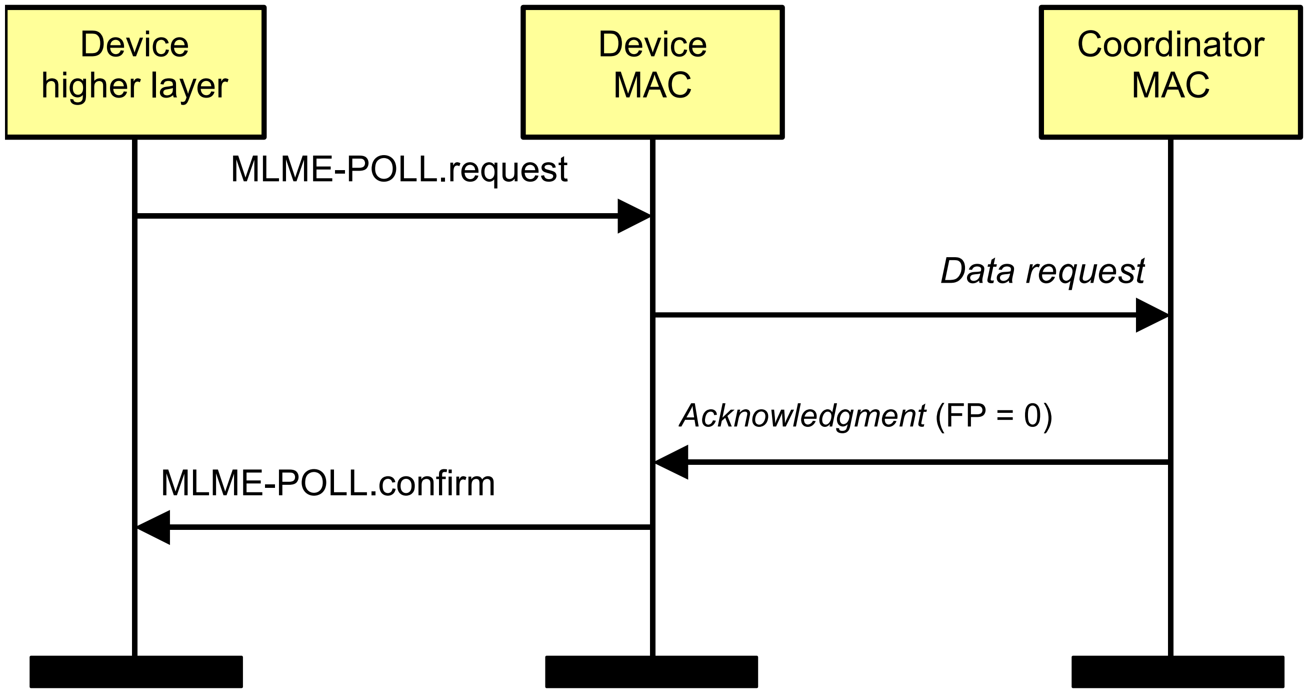
IEEE 802.15.4 MAC: Power

- Three main approaches :
  - Low power listening (LPL)
  - Scheduled contention
  - TDMA – contention free /cluster-based

IEEE 802.15.4 MAC: Low Power Listening

- Channel polling
  - Nodes wake up very briefly to check channel activity without receiving data
    - If channel idle node go back to sleep otherwise it stays awake to receive data
    - Performed regularly but not synchronised among nodes
- Rendezvous with receivers
  - Senders send a long preamble before each message to intersect with a polling

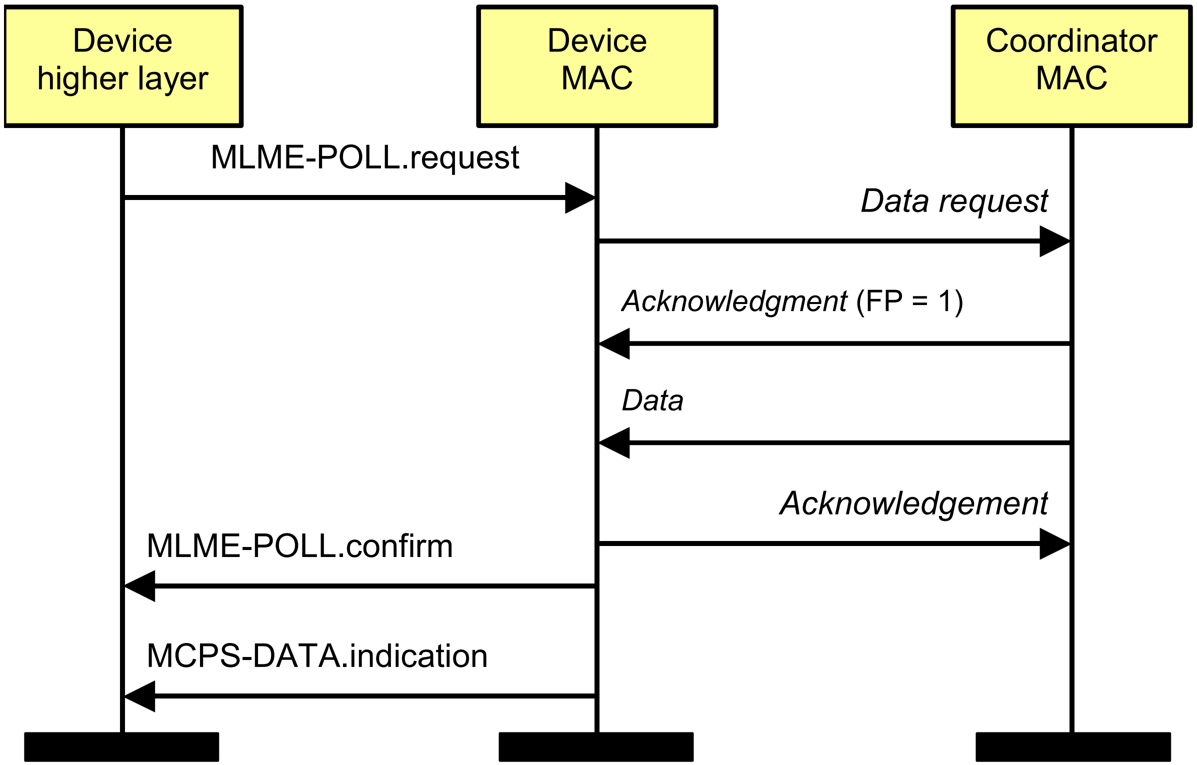
Channel Polling
Message Sequence Chart



No data pending at the coordinator

Data Polling

Message Sequence Chart



Data pending at the coordinator

IEEE 802.15.4 MAC: Low Power Listening

- Pros
  - ~ 10 times less expensive than listening for full contention period
  - Asynchronous
  - Sensitive to tuning for neighbourhood size and traffic rate
- Cons
  - Poor performance when traffic rates vary greatly. (optimised for known periodic traffic)
  - Receiver and polling efficiency is gained at the much greater cost of senders

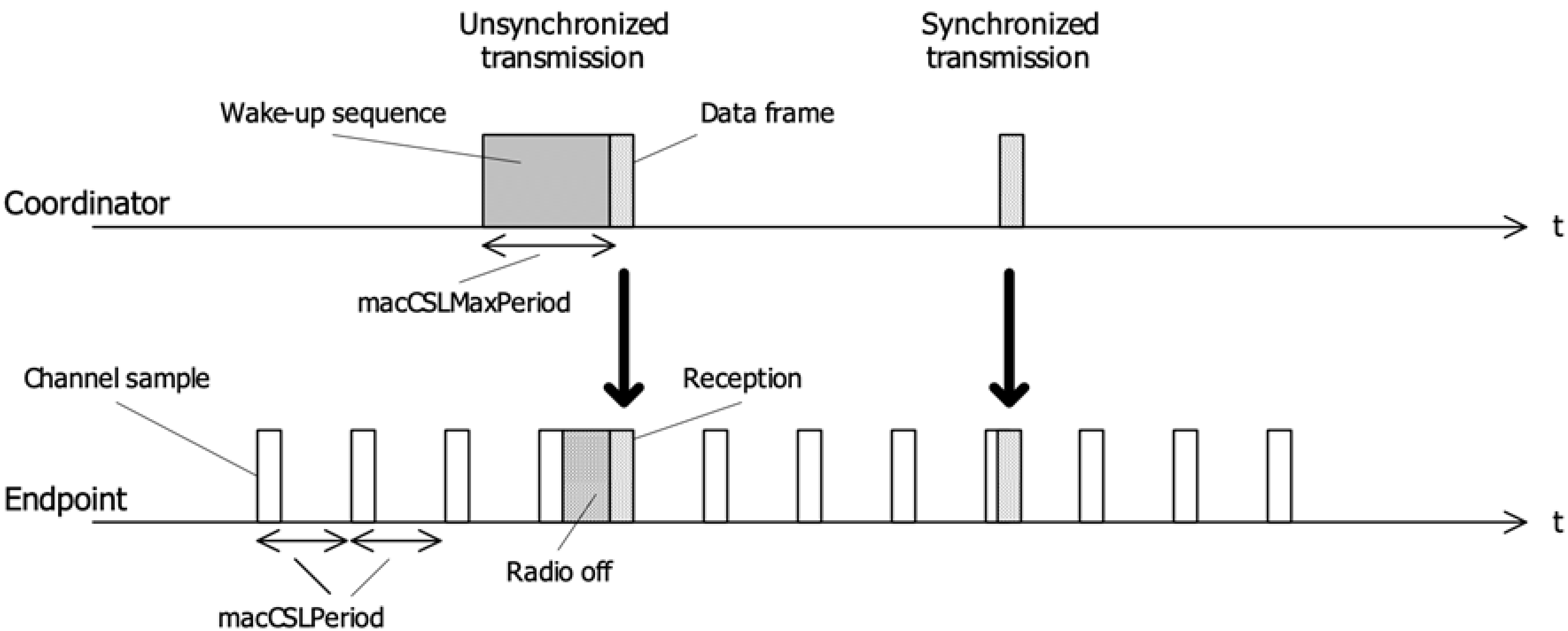
IEEE 802.15.4 MAC: Scheduled Contention

- Schedule coordinated transmission and listen periods
- Nodes adopt common schedule
- Synchronising with periodic control messages
- Receiver listen to brief contention periods while senders contend
- Only nodes participating in data transfer remain awake after contention periods while others can sleep

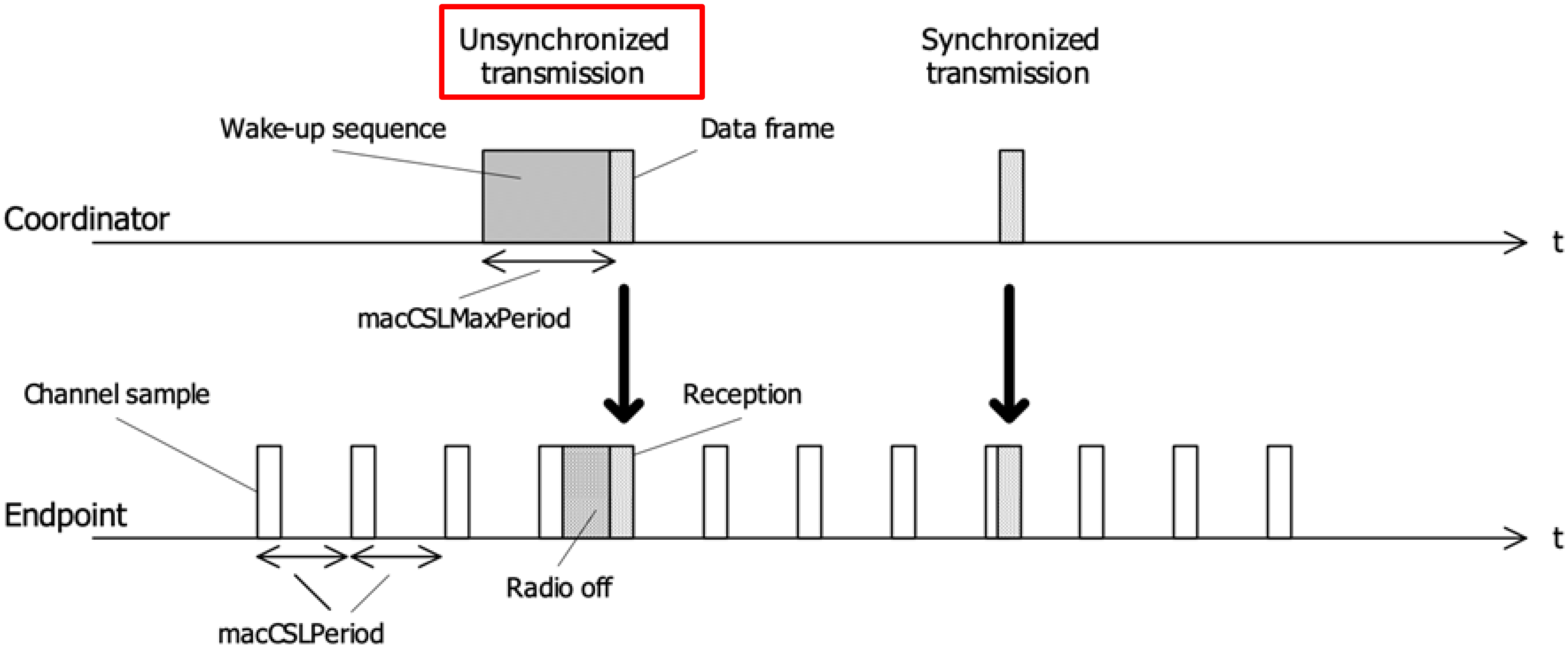
Coordinated Sampled Listening (CSL)

- Challenge:
  - How does the sender know the receiver is listening?
- Approach:
  - Start unsynchronized
  - Synchronize with wake up-sequence + ack
  - Continue data communication at synchronized times

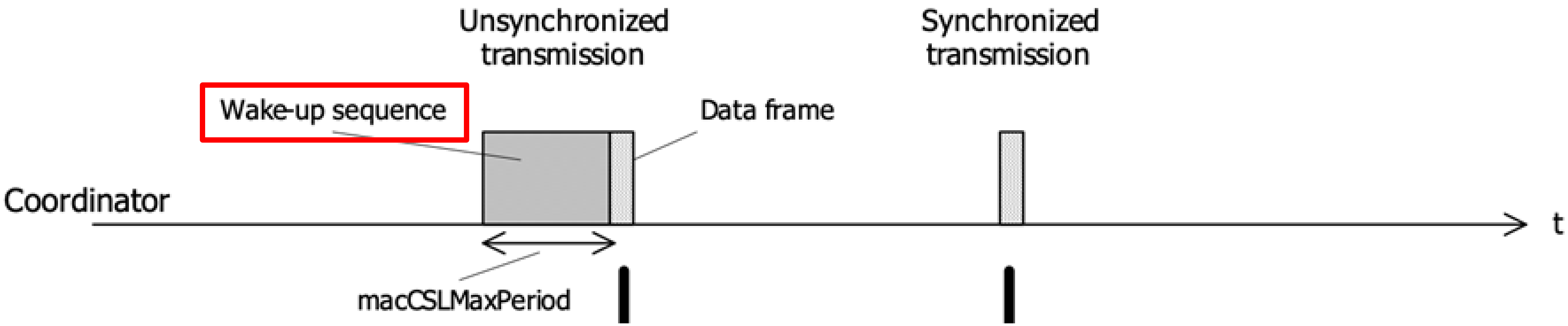
Coordinated Sampled Listening (CSL)



Coordinated Sampled Listening (CSL)

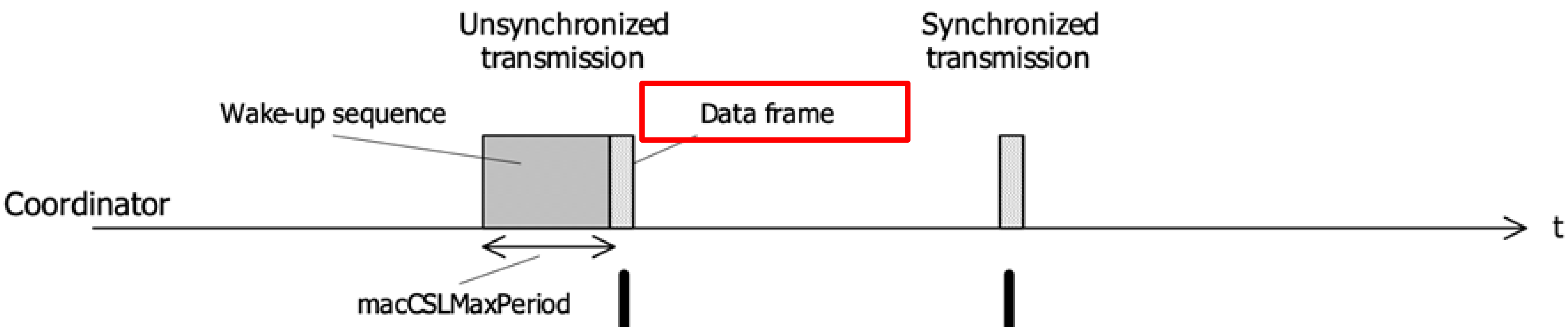


Coordinated Sampled Listening (CSL)



- Coordinator sends a sequence of wake-up frames (wake-up sequence or preamble)

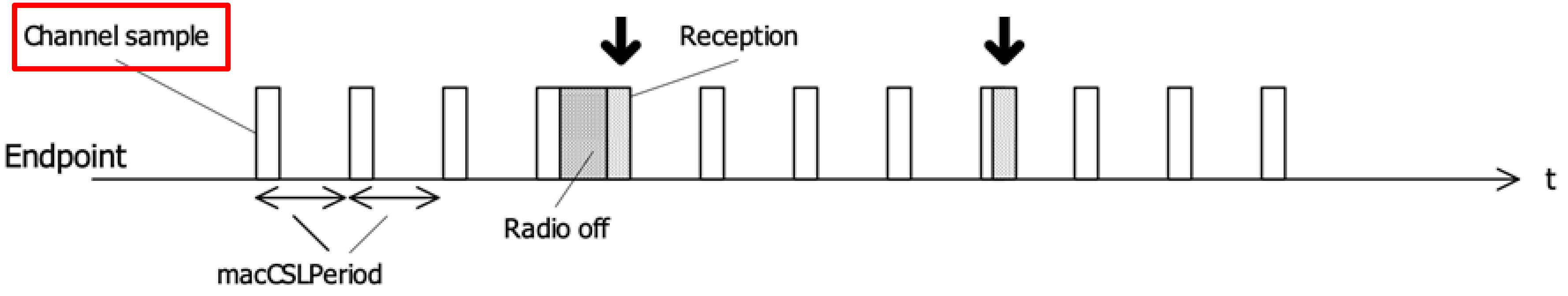
Coordinated Sampled Listening (CSL)



- Coordinator also sends a Data frame
- Wake-up frames contain timing information about when data frame arrives (Rendezvous time)

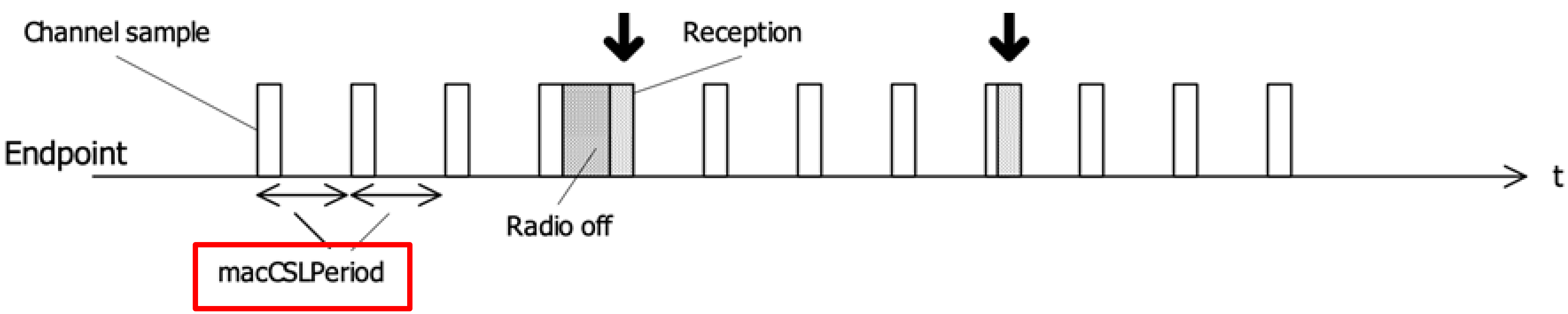
Coordinated Sampled Listening (CSL)

- Endpoint periodically samples the channel to check for wake-up frames
- If there are no wake-up frames, it goes back to sleep

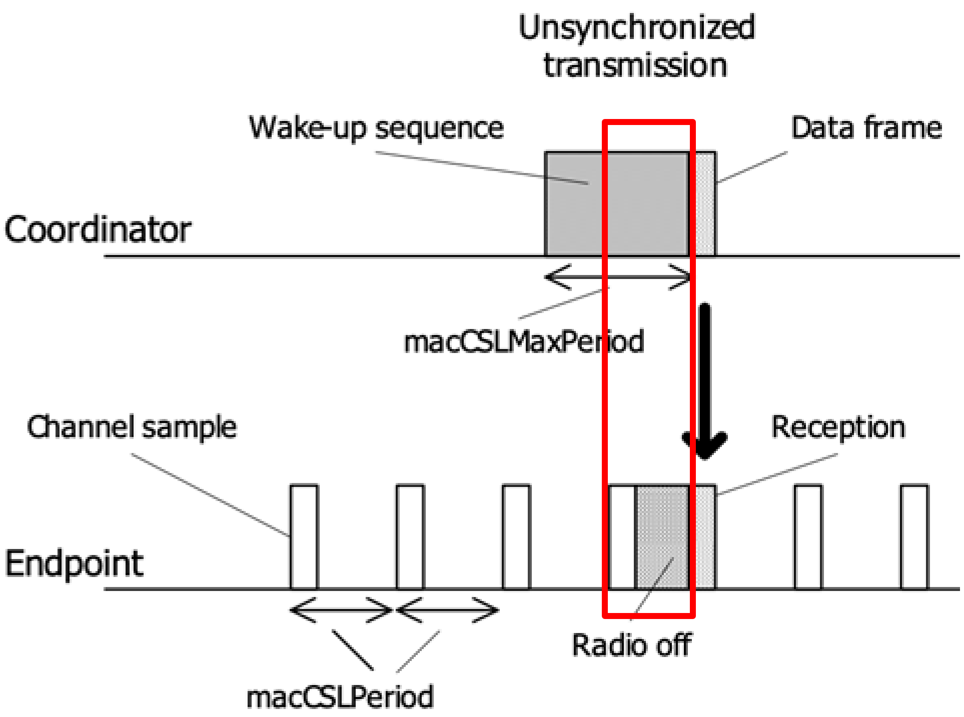


Coordinated Sampled Listening (CSL)

- Endpoint periodically samples the channel to check for wake-up frames
- If there are no wake-up frames, it goes back to sleep
- Samples occur every macCSLPeriod



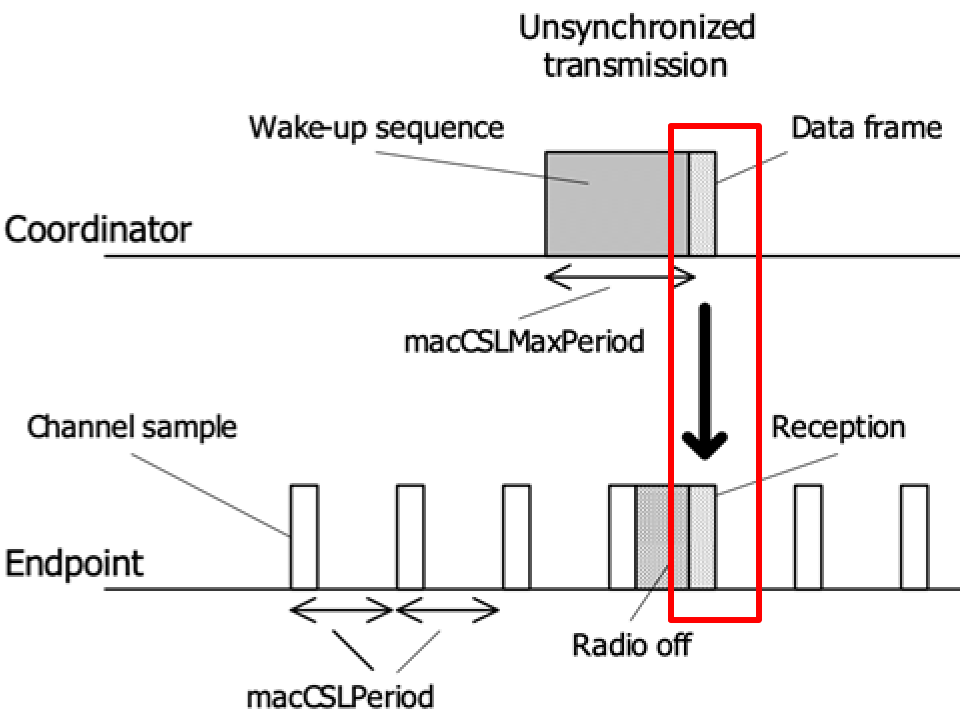
Coordinated Sampled Listening (CSL)



- Upon sampling wake-up frame, Endpoint retrieves Rendezvous time for data
- Sleeps until Rendezvous time

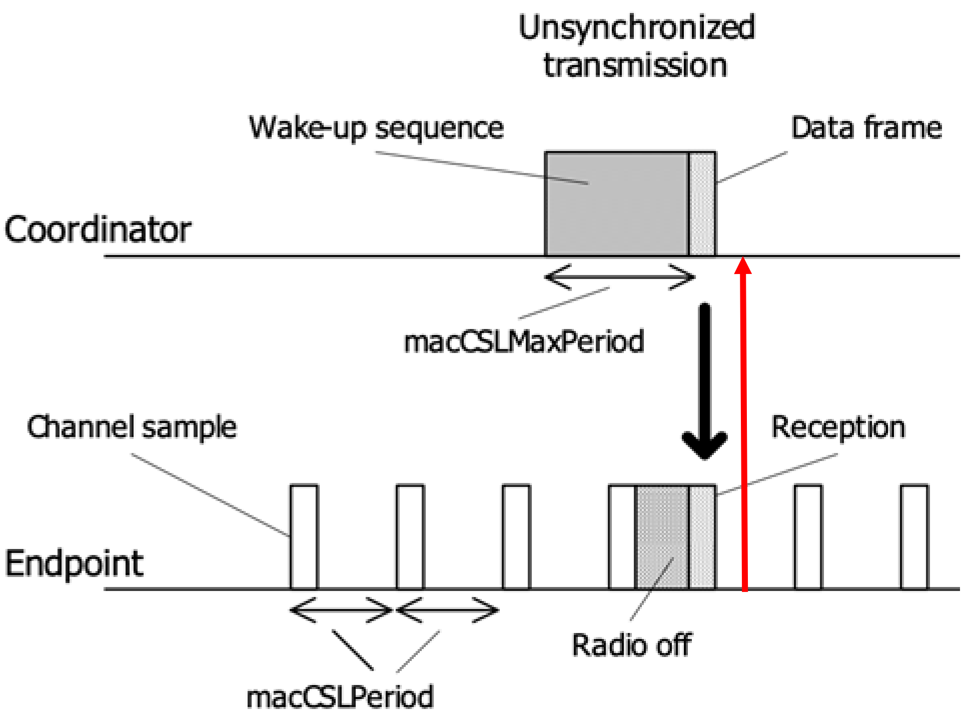
Octets: 2	2
Rendezvous Time	Wake-up Interval

Coordinated Sampled Listening (CSL)



- Upon sampling wake-up frame, Endpoint retrieves Rendezvous time for data
- Sleeps until Rendezvous time
- Retrieves data frame at Rendezvous time

Coordinated Sampled Listening (CSL)



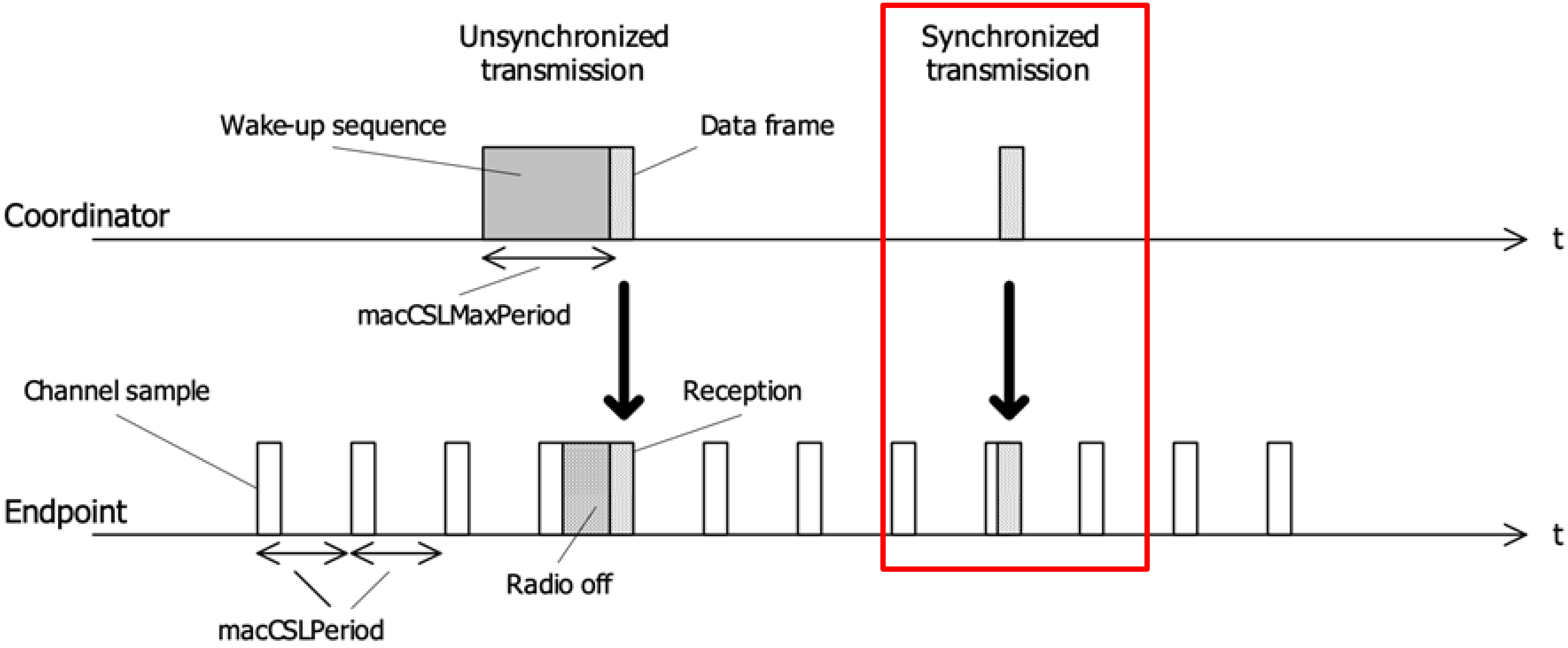
- Upon sampling wake-up frame, Endpoint retrieves Rendevous time for data
- Sleeps until Rendevous time
- Retrieves data frame at Rendezvous time
- Ack's back CSL period and CSL Phase

Coordinated Sampled Listening (CSL)

Octets: 2	2	0/2
CSL Phase	CSL Period	Rendezvous Time

- CSL Phase: Time between coordinator transmissions
- CSL Period: Time between receiver samples

Coordinated Sampled Listening (CSL)



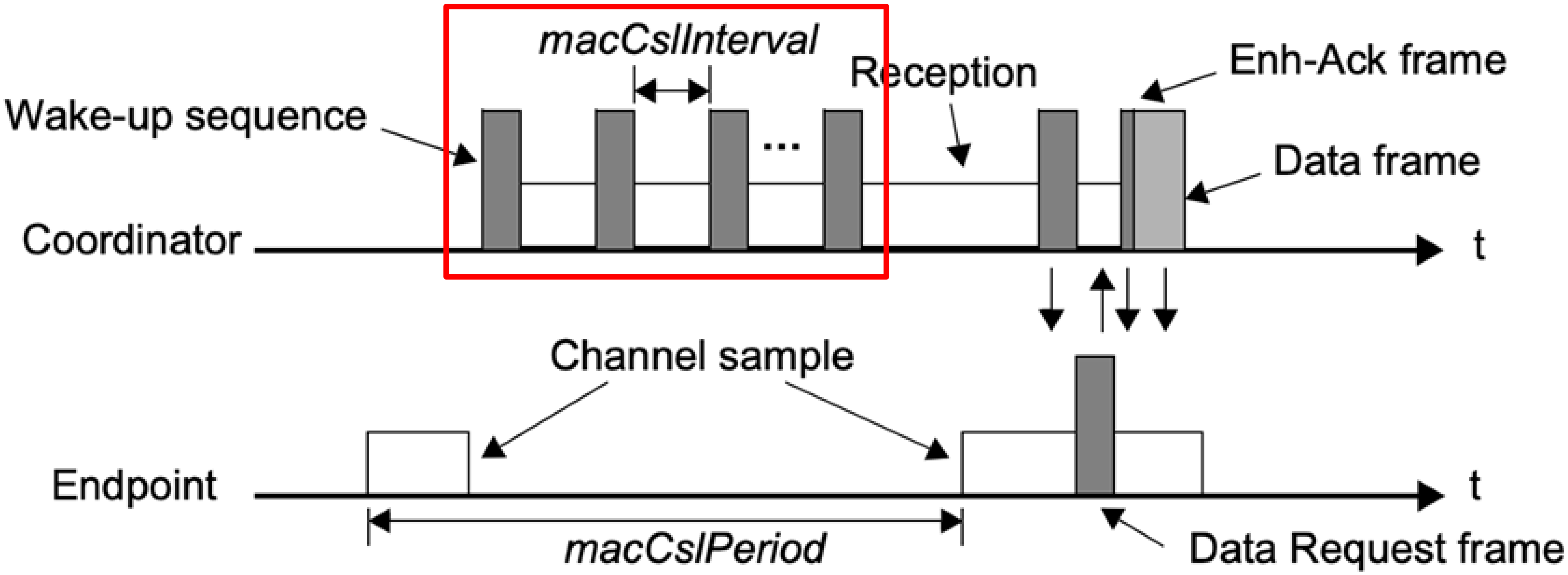
Coordinated Sampled Listening (CSL)

- What if Wake-up interval is nonzero?

Octets: 2	**2**
Rendezvous Time	Wake-up Interval

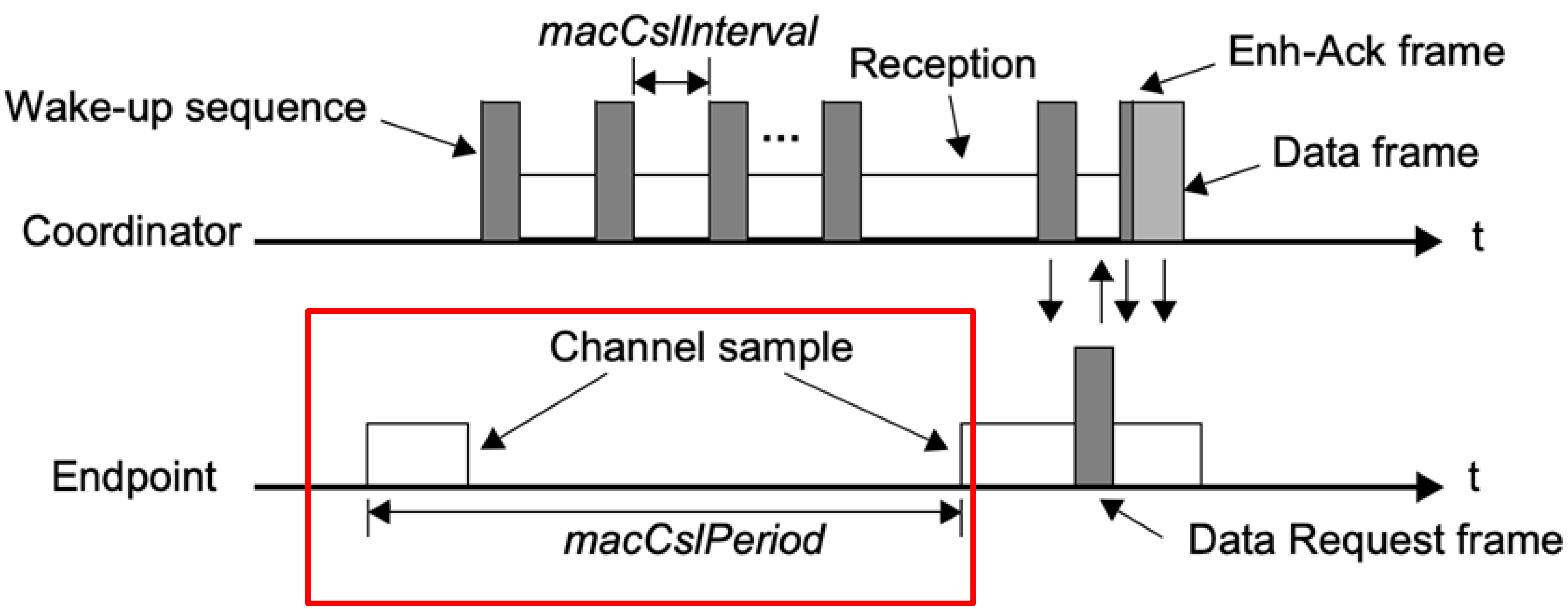
Coordinated Sampled Listening (CSL)

- Wake-up interval nonzero:



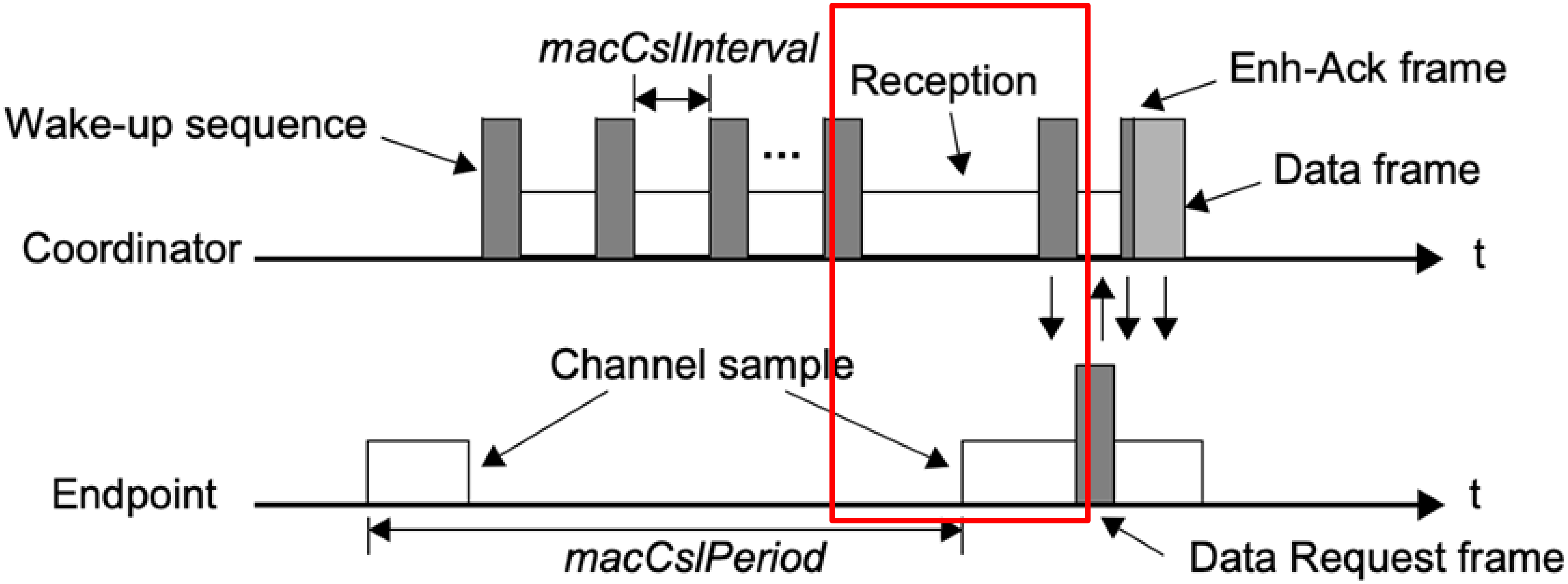
Coordinated Sampled Listening (CSL)

- Wake-up interval nonzero:



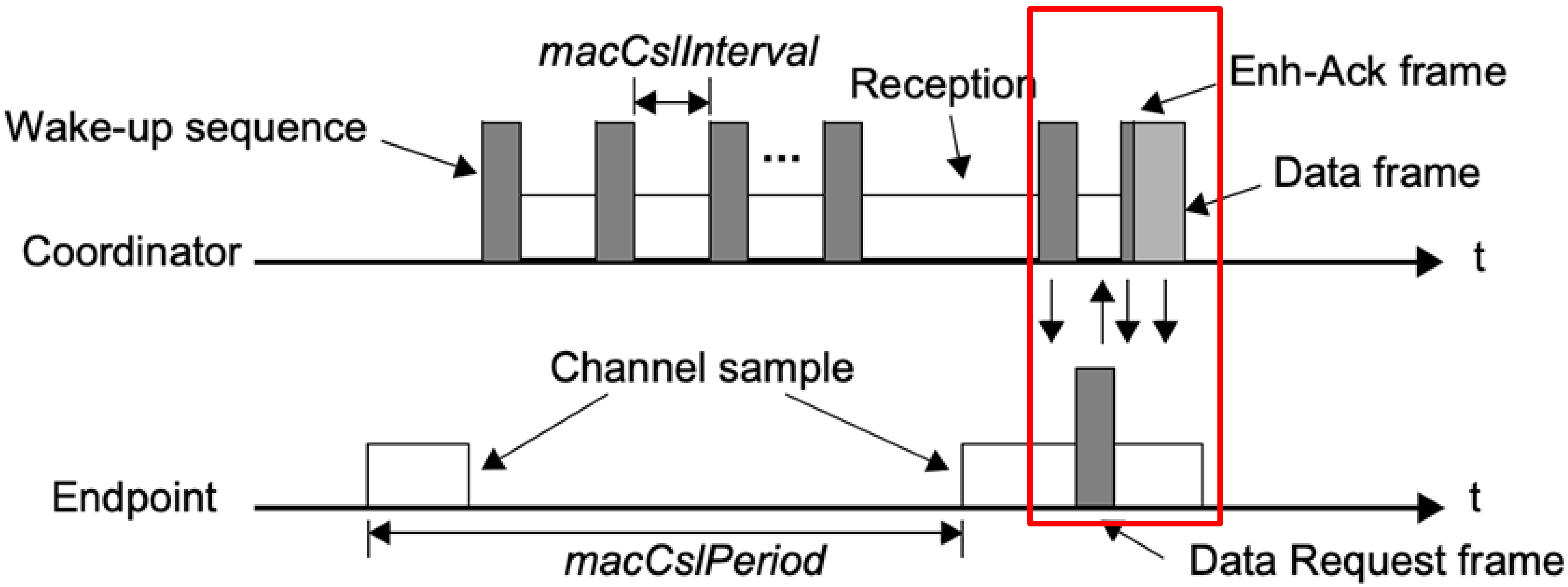
Coordinated Sampled Listening (CSL)

- Wake-up interval nonzero:



Coordinated Sampled Listening (CSL)

- Wake-up interval nonzero:



IEEE 802.15.4 MAC: Scheduled Contention

- Pros
  - Improved performance with traffic increase
  - similar cost incurred by sender and receiver
  - Scalable, adaptive and flexible
- Cons
  - Listening for full contention period
  - Synchronous
  - Sensitive to clock drift

IEEE 802.15.4 MAC: TDMA

- Allocation of time slots by base station (BS)/cluster head (CH)
- Only one node is allowed to transmit in a slot
- Timing and synchronisation provided by BS/CH
- Normally require nodes to form clusters with one node as CH/BS
- Communication between nodes and cluster head; no peer to peer communication

IEEE 802.15.4 MAC: TDMA

- Pros
  - Low duty cycle
- Cons
  - Synchronous
  - Fine grained time synchronisation
  - Very sensitive to clock drift
  - Limited throughput and number of active nodes
  - Require clustering >>cost incurred more on Cluster head
  - Limited scalability and adaptivity to changes on number of nodes