

CS 439: Wireless Networking

IEEE 802.15.4/ZigBee

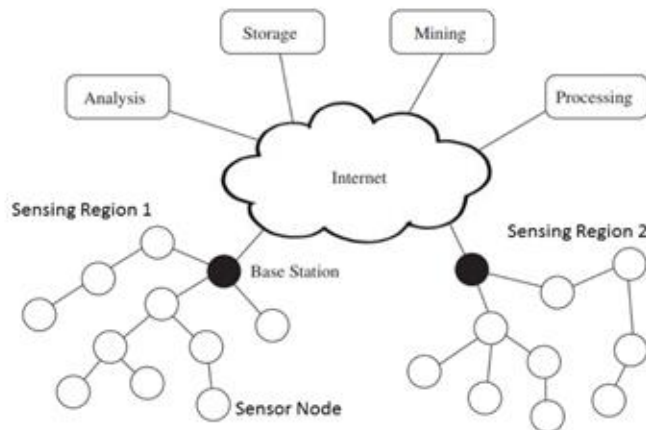
IEEE 802.15.4 Motivation

- ▶ Wi-Fi was too heavyweight
- ▶ Bluetooth was too complex
- ▶ No suitable protocol for large low-power meshes



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



Zigbee vs 802.15.4

▶ IEEE 802.15.4

- ▶ Released in 2003
- ▶ Defines MAC and PHY layer
- ▶ Low Data Rate, Low Power

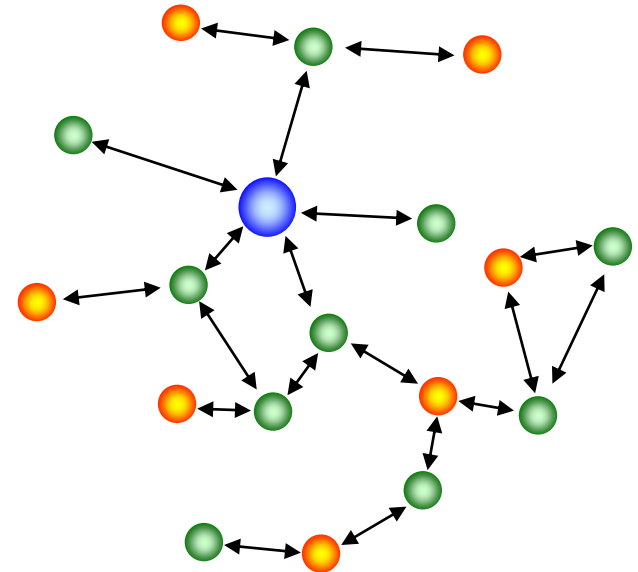
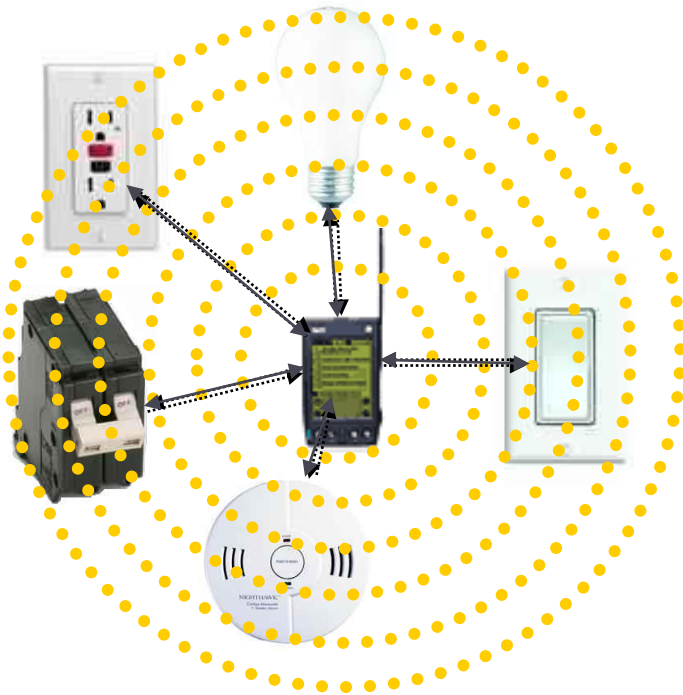


▶ ZigBee

- ▶ Released in 2005
- ▶ Defines Network Layer and above on top of 802.15.4

802.15.4 Applications Space

- ▶ Home Networking
- ▶ Industrial Networks
- ▶ Healthcare/Medical applications
- ▶ Interactive Toys
- ▶ Remote Metering

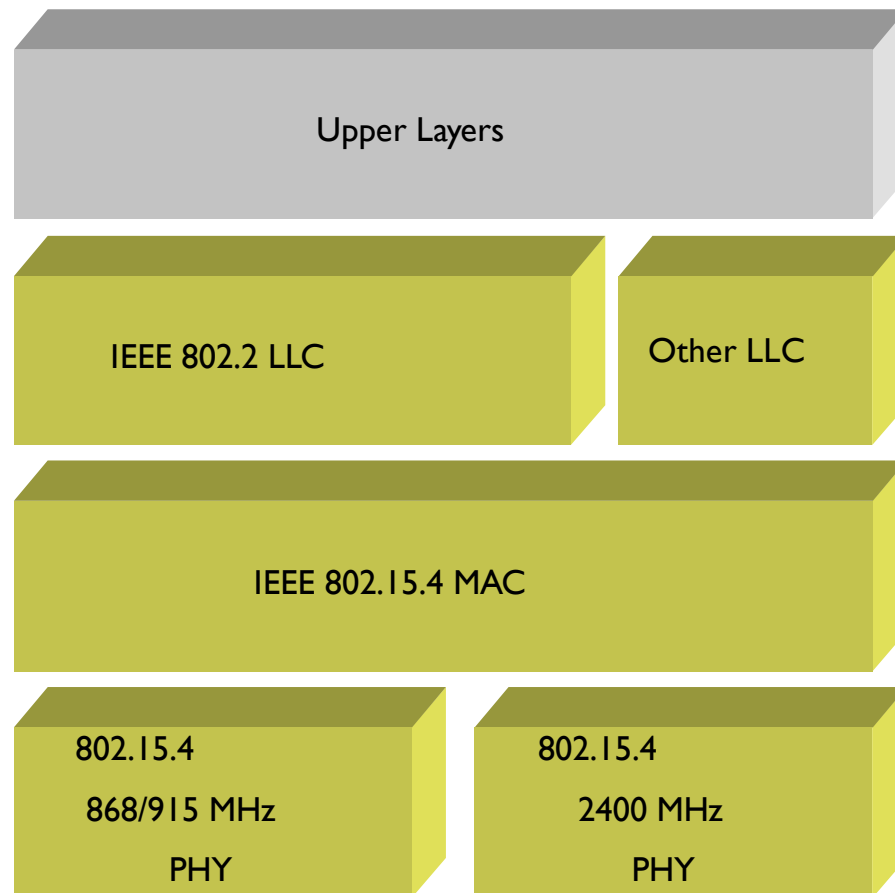


802.15.4 General Characteristics

- ▶ Star or Peer-to-Peer Network Topology
- ▶ CSMA/CA channel access
- ▶ Dynamic device addressing
- ▶ Fully handshaked protocol for transfer reliability
- ▶ Range about 10–100 m
- ▶ Low power consumption



802.15.4 Architecture



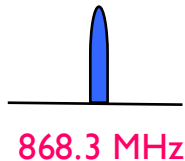
- **Frequency bands**
- **Modulation/spreading**



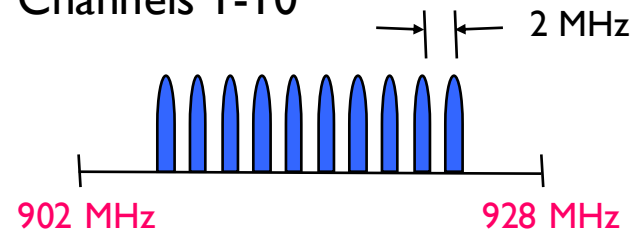
IEEE 802.15.4 PHY: Frequency Bands

868MHz / 915MHz PHY

Channel 0

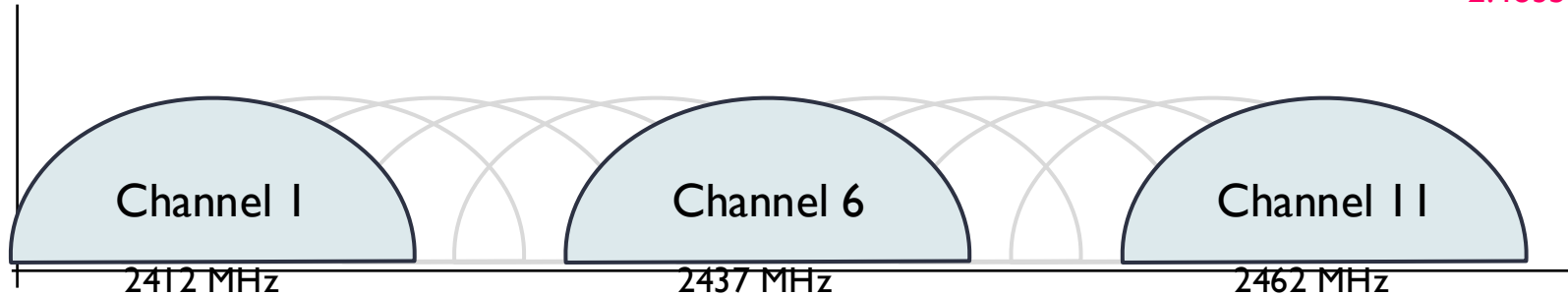
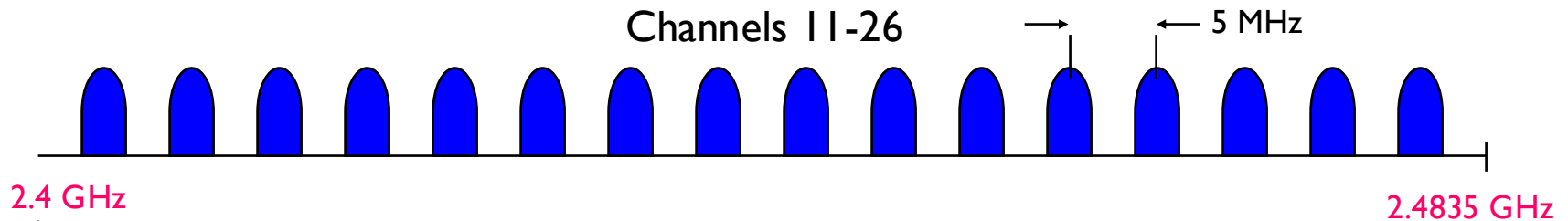


Channels 1-10



2.4 GHz PHY

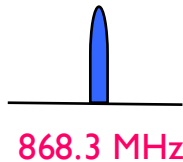
Channels 11-26



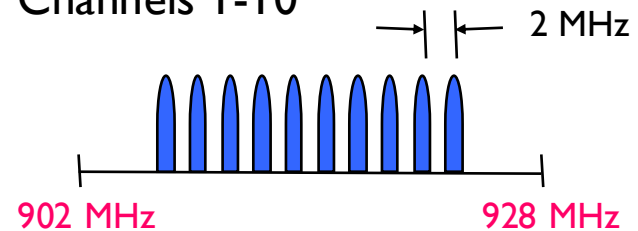
IEEE 802.15.4 PHY: Frequency Bands

**868MHz /
915MHz
PHY**

Channel 0

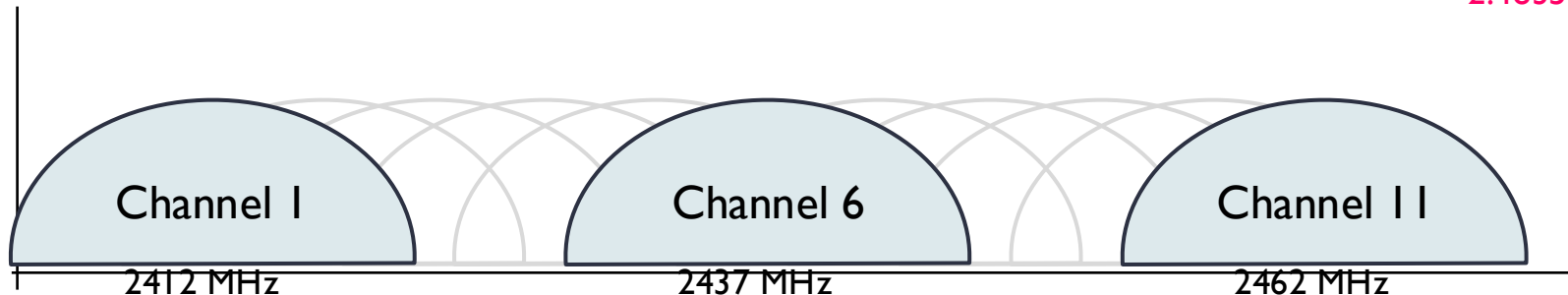
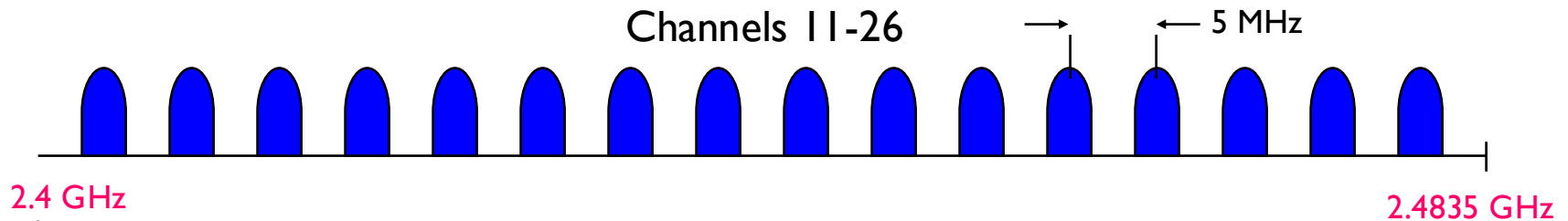


Channels 1-10



2.4 GHz PHY

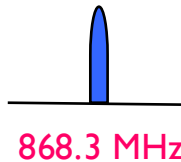
Channels 11-26



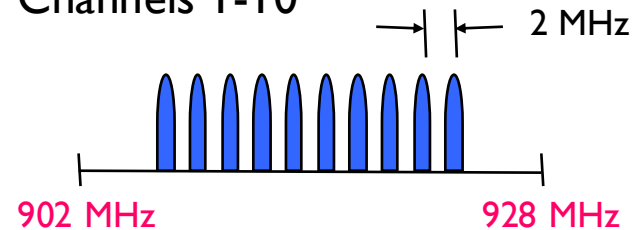
IEEE 802.15.4 PHY: Frequency Bands

**868MHz /
915MHz
PHY**

Channel 0

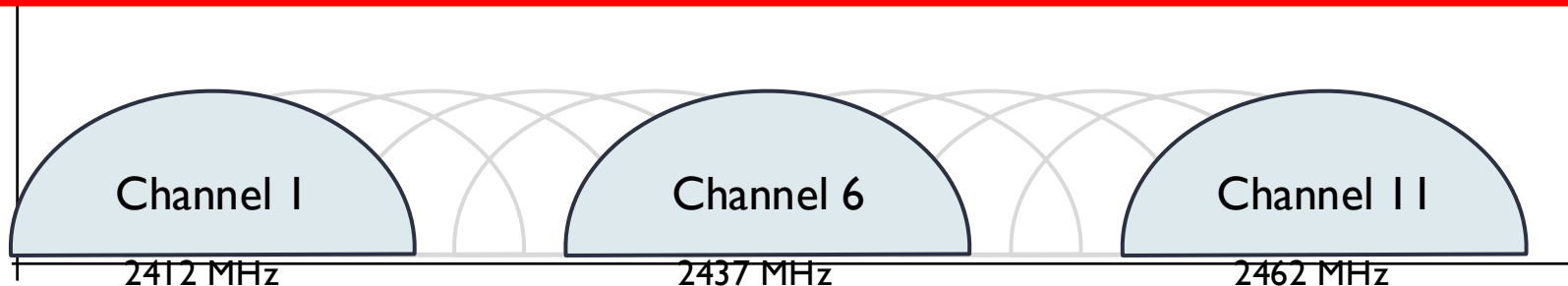
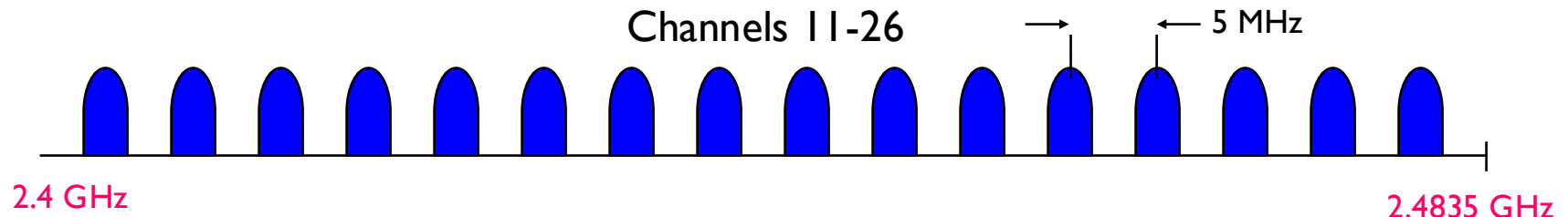


Channels 1-10



2.4 GHz PHY

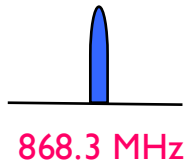
Channels 11-26



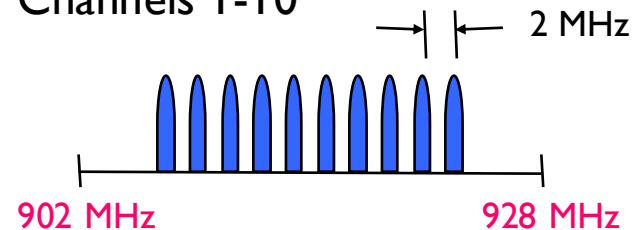
IEEE 802.15.4 PHY: Frequency Bands

868MHz / 915MHz PHY

Channel 0



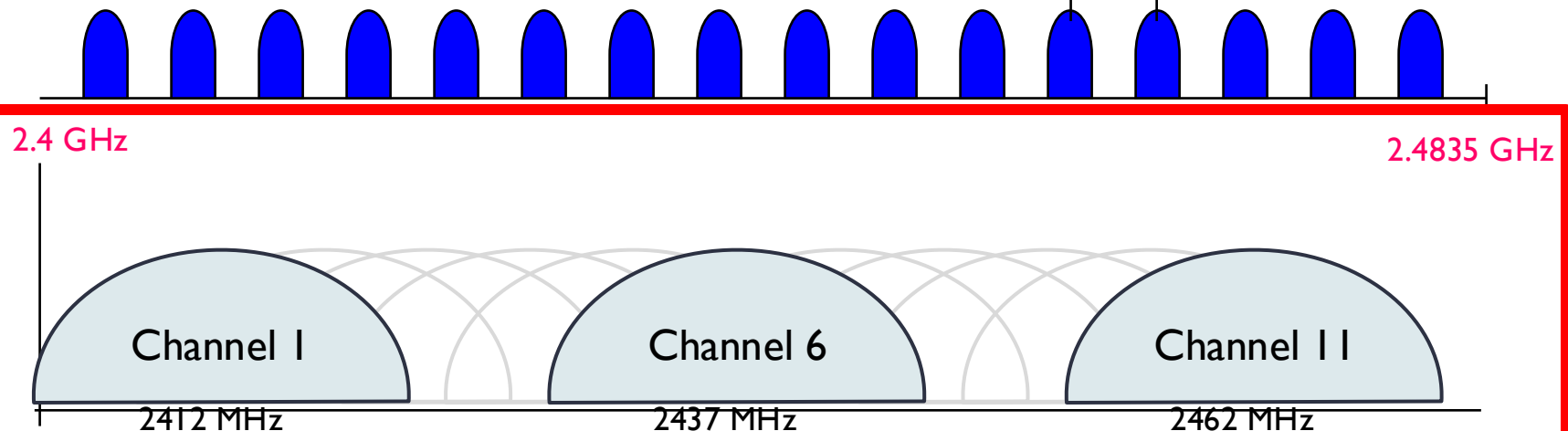
Channels 1-10



2.4 GHz PHY

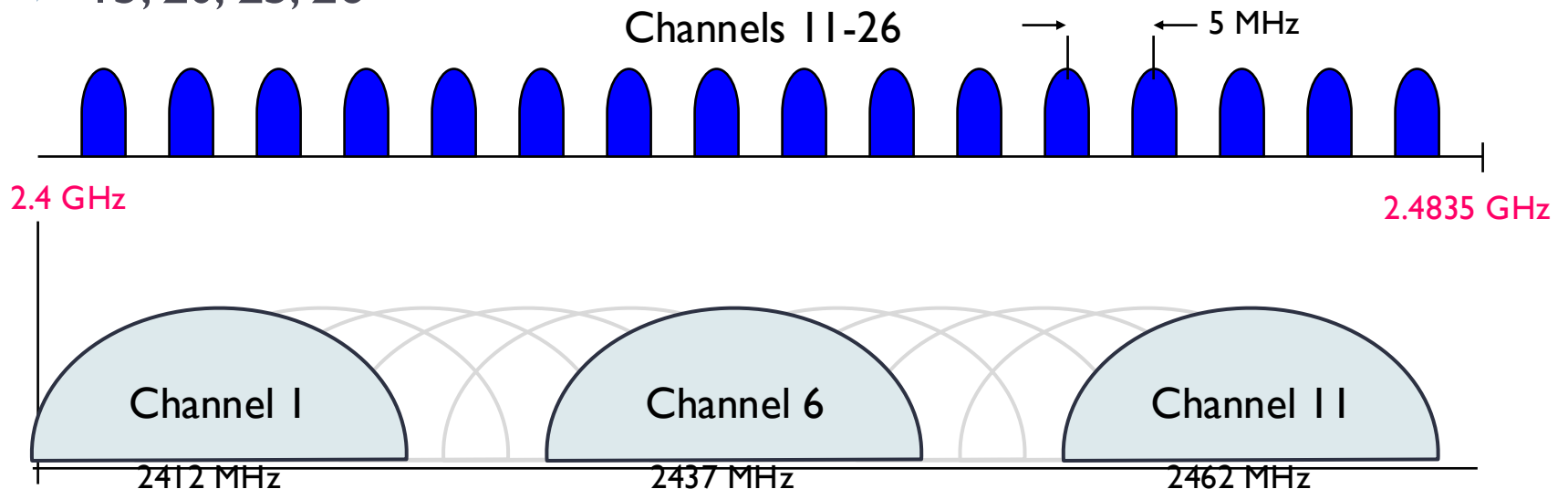
Channels 11-26

5 MHz



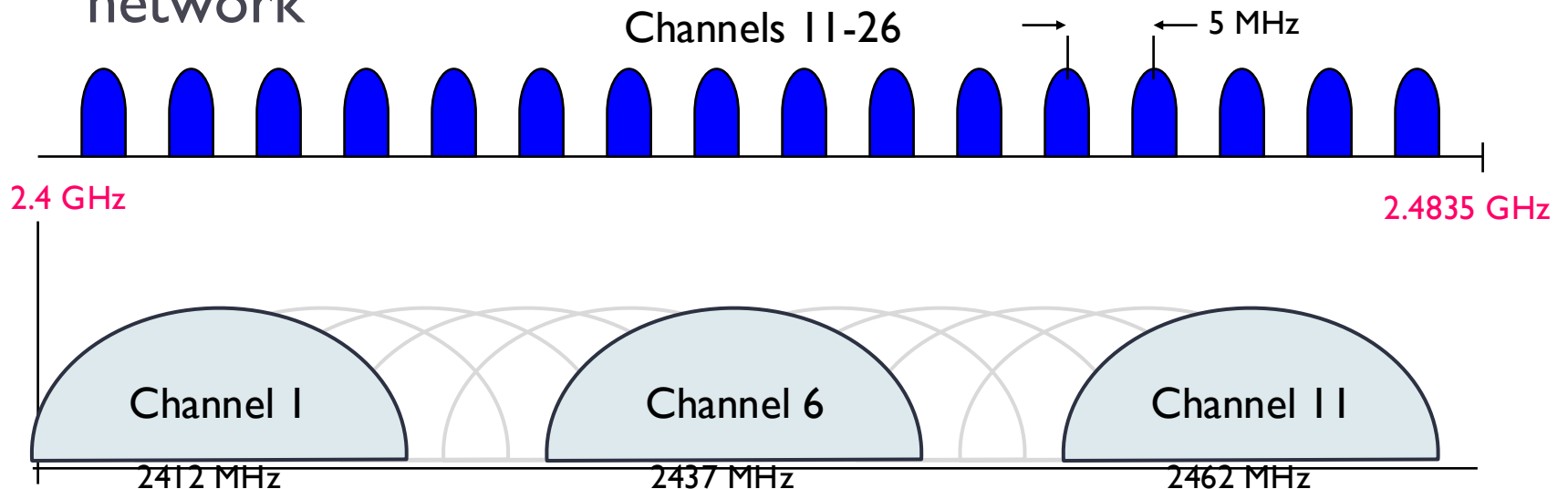
802.15.4 and Wi-Fi Coexistence

- ▶ Wi-Fi channels 1, 6, 11
 - ▶ Centers 2412, 2437, 2462 MHz, about 20 MHz wide
- ▶ 802.15.4 channels 11–26
 - ▶ 2 MHz wide, 5 MHz apart
 - ▶ Center = $2405 + 5 \times (k - 11)$ MHz
- ▶ Channels that fall in the gaps between Wi-Fi 1/6/11
 - ▶ 15, 20, 25, 26



802.15.4 and Wi-Fi Coexistence

- ▶ Wi-Fi is wider and much stronger, so 802.15.4 is usually the victim
- ▶ Coordinator picks a channel using an energy scan at network formation
 - ▶ Later Wi-Fi channel changes can still break a 802.15.4 network

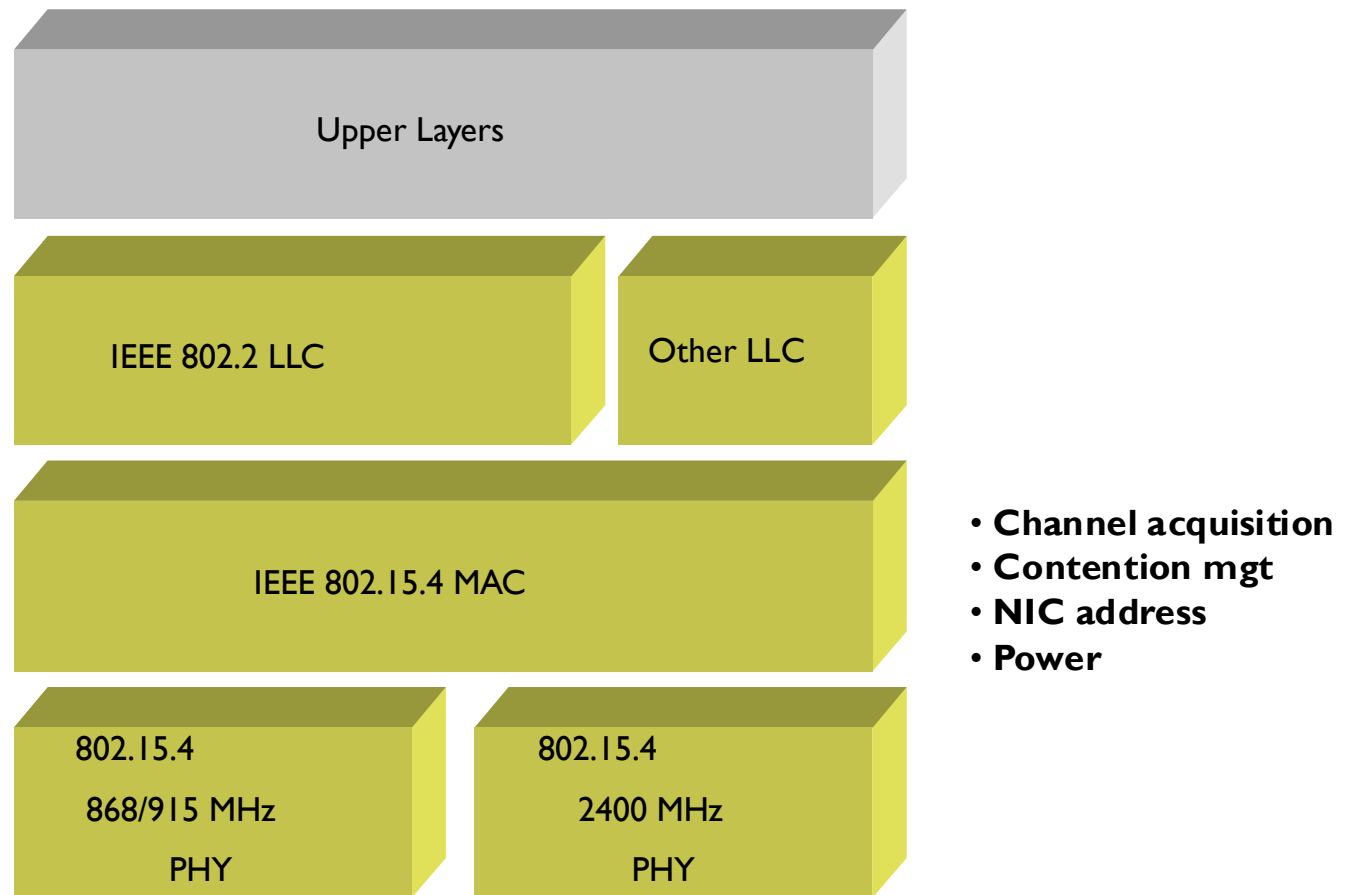


802.15.4 Physical Layers

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 Architecture



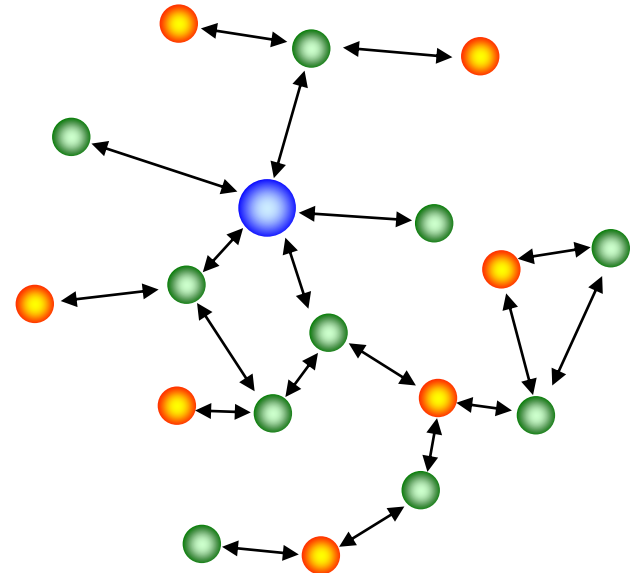
IEEE 802.15.4 MAC: Design Drivers

- ▶ 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

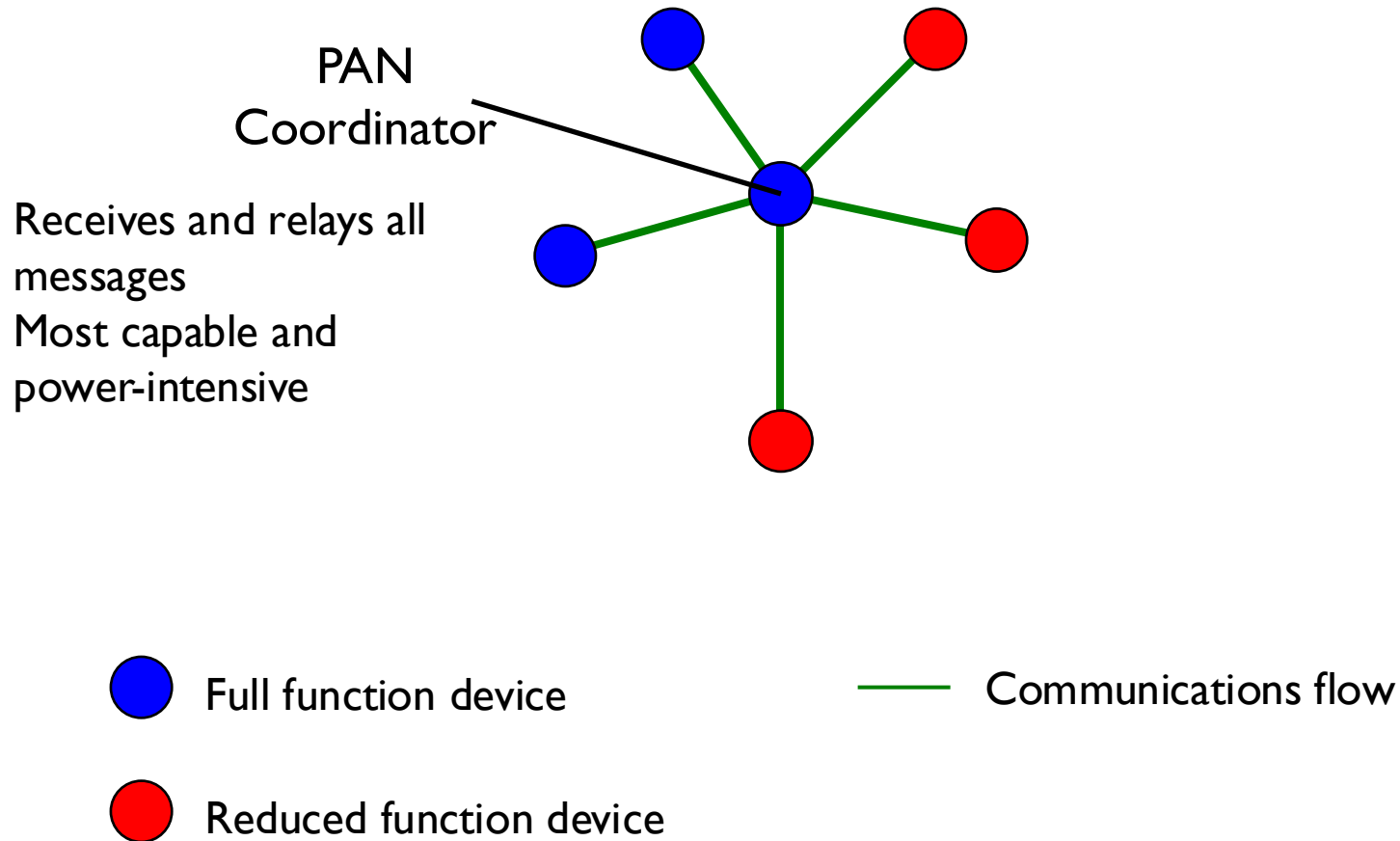


IEEE 802.15.4 MAC: Device Classes

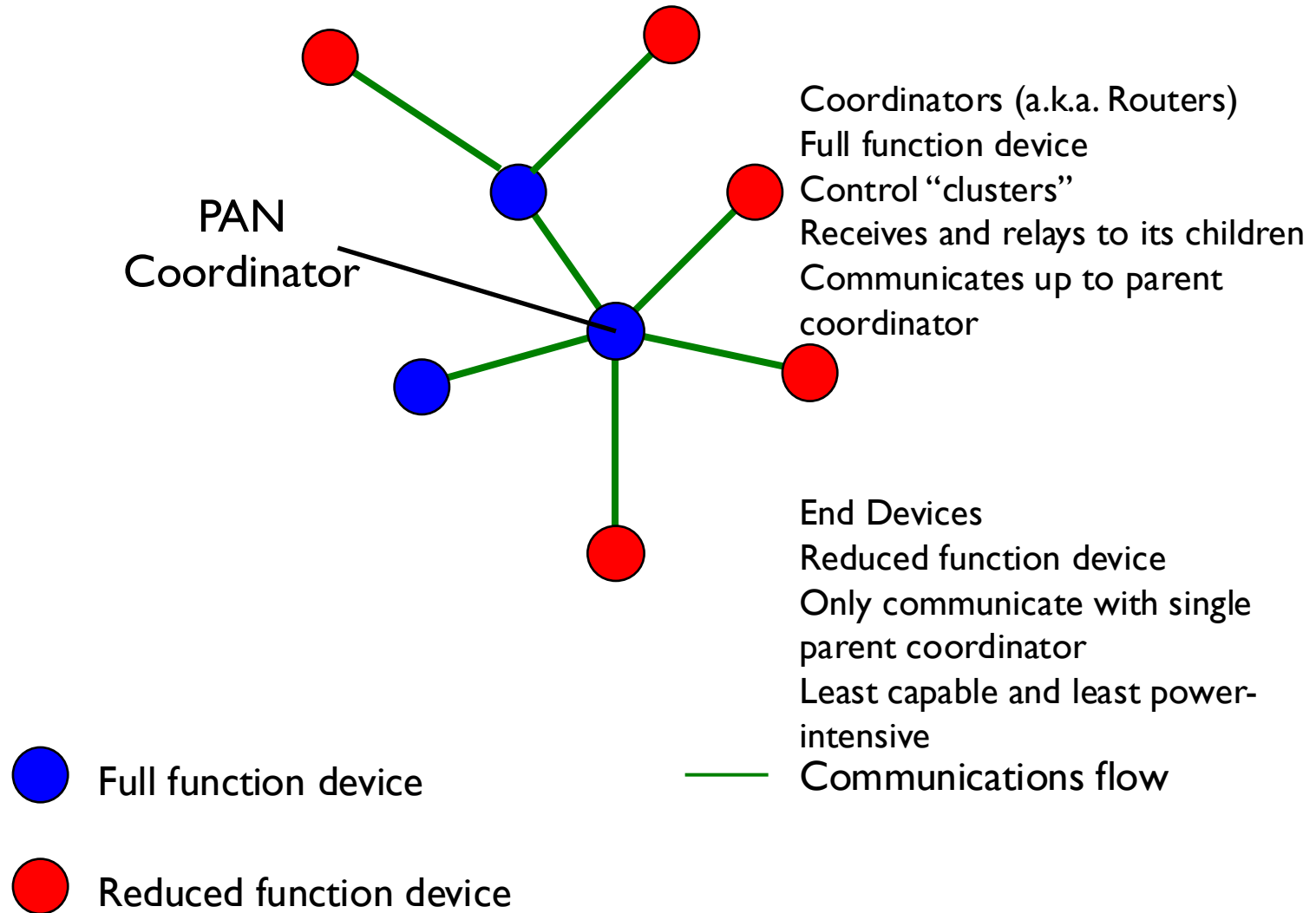
- ▶ **Full function device (FFD)**
 - ▶ Any topology
 - ▶ Network coordinator capable
 - ▶ Talks to any other device
- ▶ **Reduced function device (RFD)**
 - ▶ Limited to star topology
 - ▶ Cannot become a network coordinator
 - ▶ Talks only to a network coordinator
 - ▶ Very simple implementation



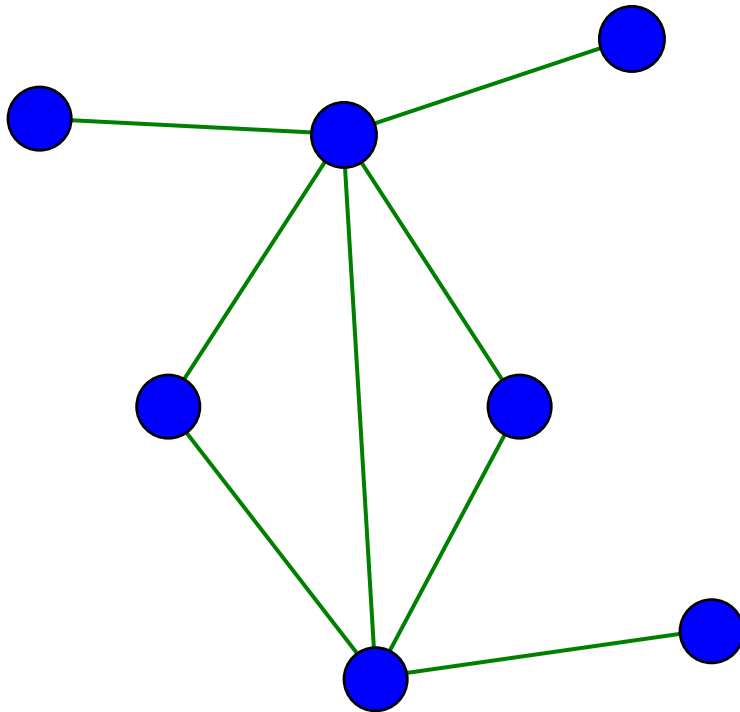
IEEE 802.15.4 MAC: Star Topology



IEEE 802.15.4 MAC: Tree Topology

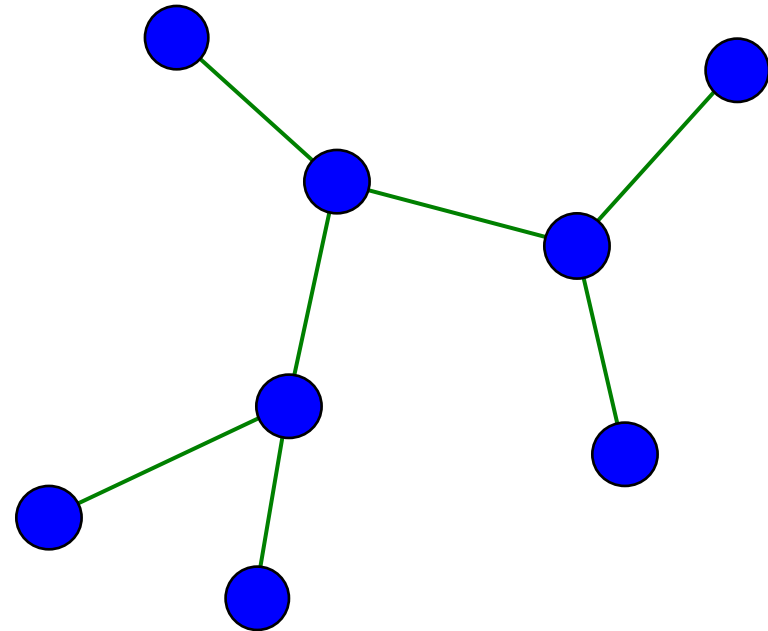


IEEE 802.15.4 MAC: Peer-Peer Topology



Point to point

● Full function device



Cluster tree

— Communications flow

Figure 1. The effect of the concentration of the *Agrobacterium* strain on the transformation efficiency of *Agrobacterium* strain.

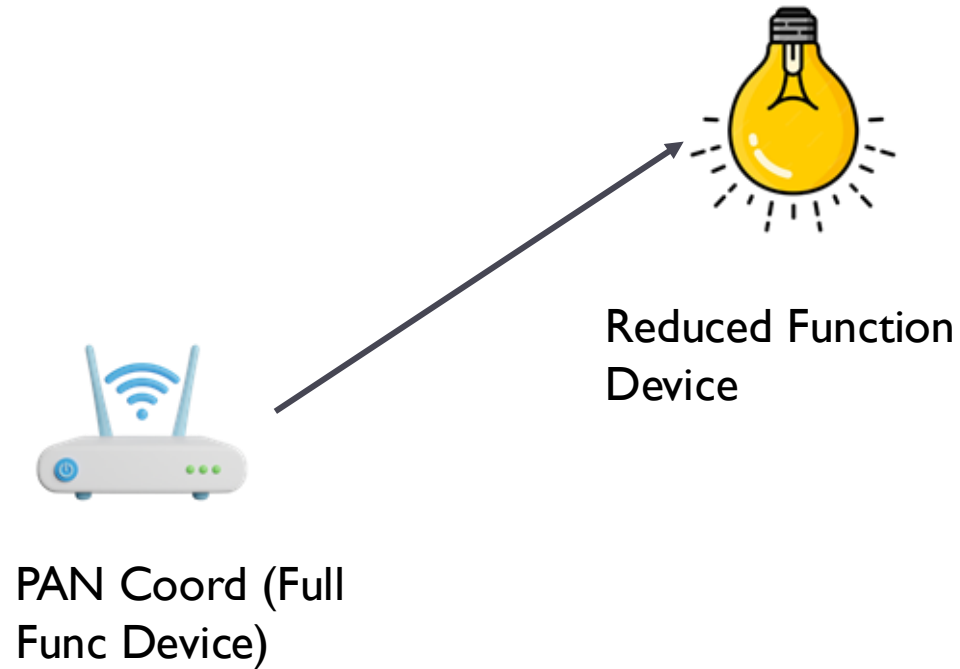
- Full function device

Network Example

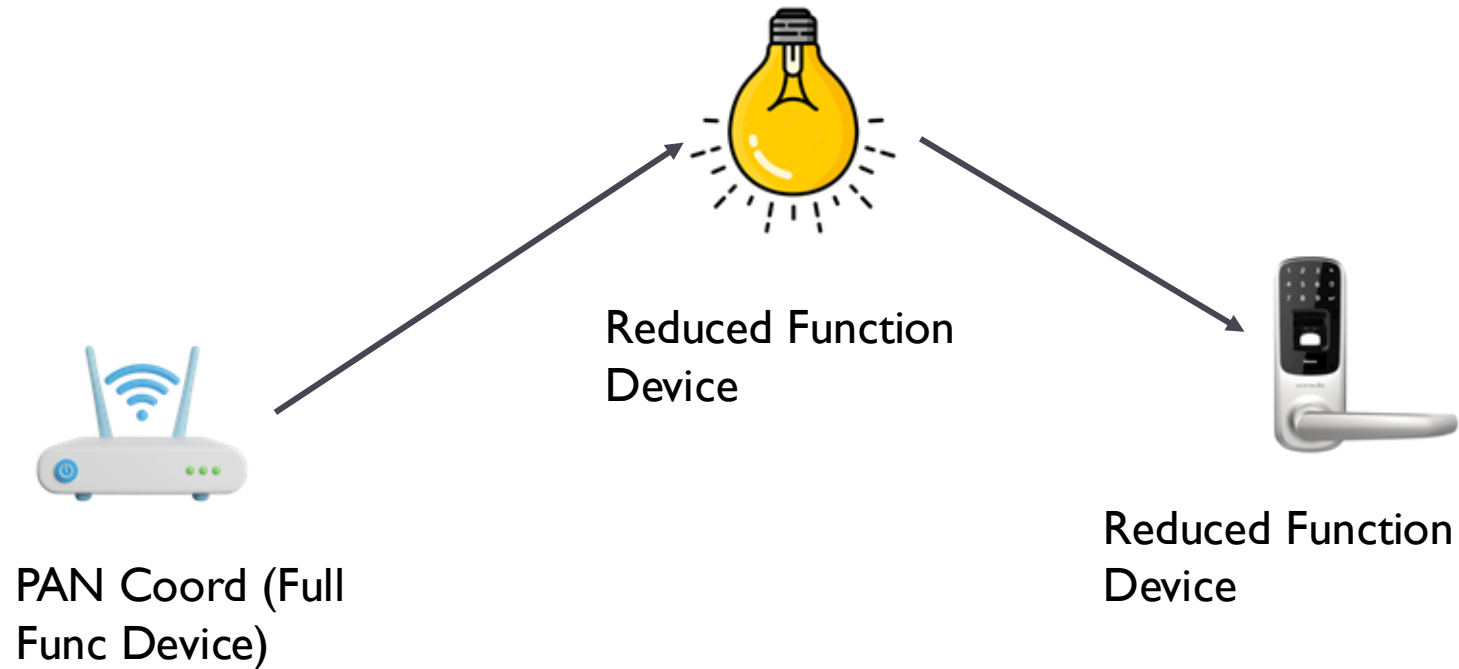


PAN Coord (Full
Func Device)

Network Example



Network Example



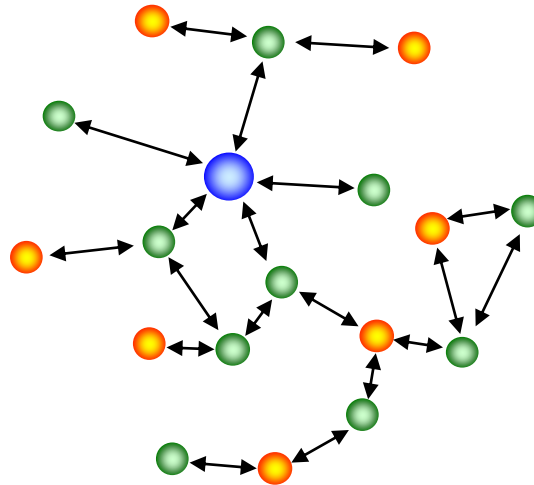
IEEE 802.15.4 MAC: Traffic Types

- ▶ **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)



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)



802.15.4 MAC: Medium Access

- ▶ Unslotted (vanilla CSMA/CA, no beacons)
 - ▶ Random backoff, then clear channel assessment (CCA)
 - ▶ backoffs = 0, BE = macMinBE (default 3)
 - ▶ CCA idle: transmit. CCA busy: backoffs++, BE = min(BE + 1, 5), retry
 - ▶ Backoffs exceed macMaxCSMABackoffs (default 4): report channel access failure
- ▶ Slotted (beacon-enabled)
 - ▶ Backoffs align to superframe slot boundaries; two CCAs required

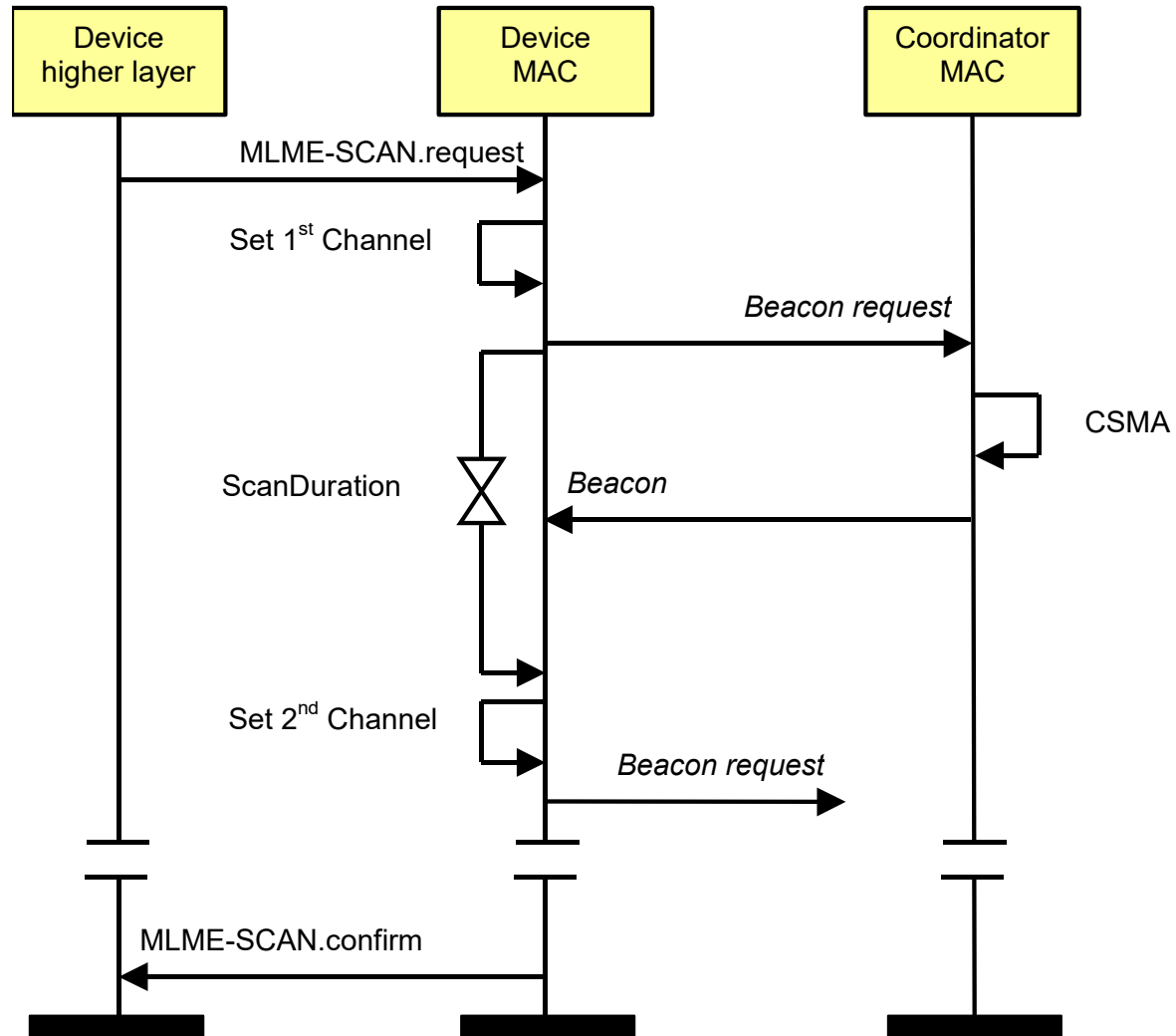


802.15.4 MAC: Medium Access

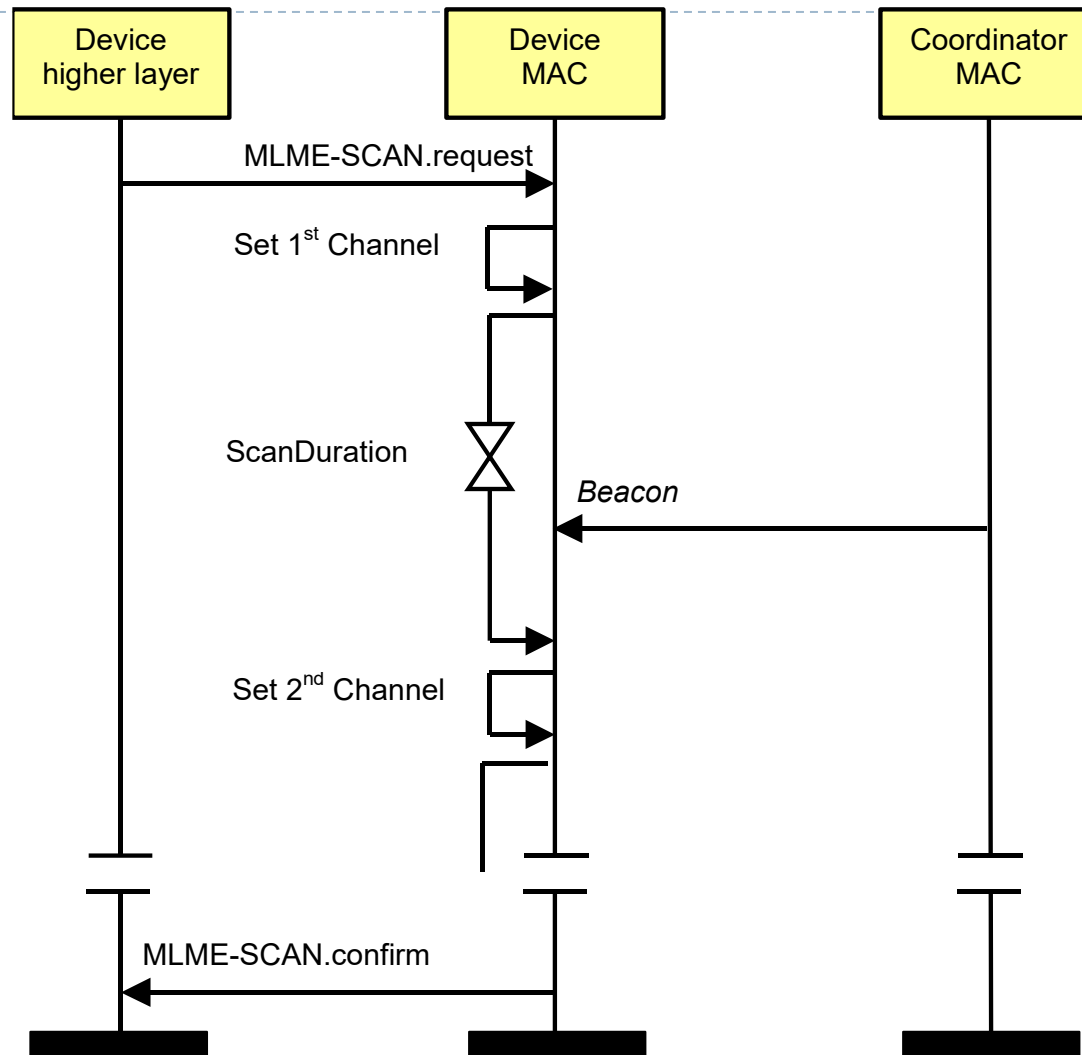
- ▶ Unslotted (vanilla CSMA/CA, no beacons)
 - ▶ Random backoff, then clear channel assessment (CCA)
 - ▶ backoffs = 0, BE = macMinBE (default 3)
 - ▶ CCA idle: transmit. CCA busy: backoffs++, BE = min(BE + 1, 5), retry
 - ▶ Backoffs exceed macMaxCSMABackoffs (default 4): report channel access failure
- ▶ Slotted (beacon-enabled)
 - ▶ Backoffs align to superframe slot boundaries; two CCAs required
- ▶ Acknowledged frames are retried up to macMaxFrameRetries (default 3)
- ▶ No RTS/CTS and no carrier-sense on beacons or GTS slots



Active Scan

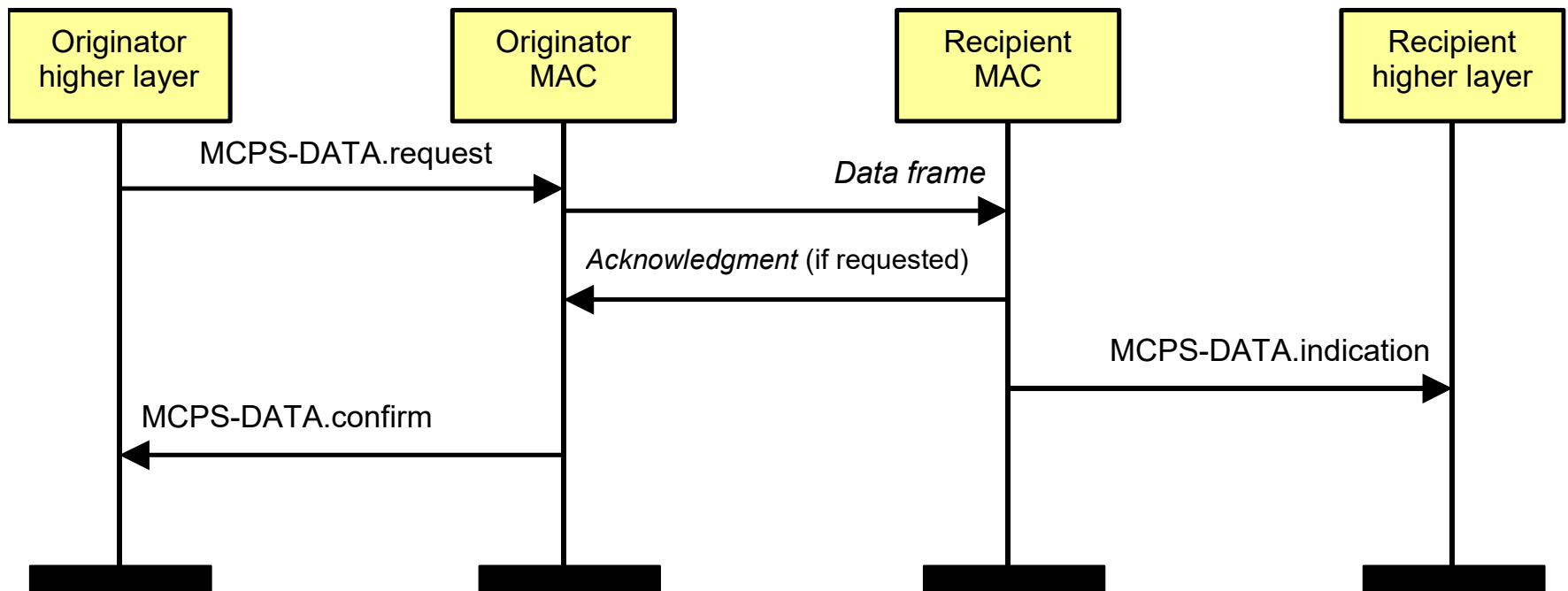


Passive Scan

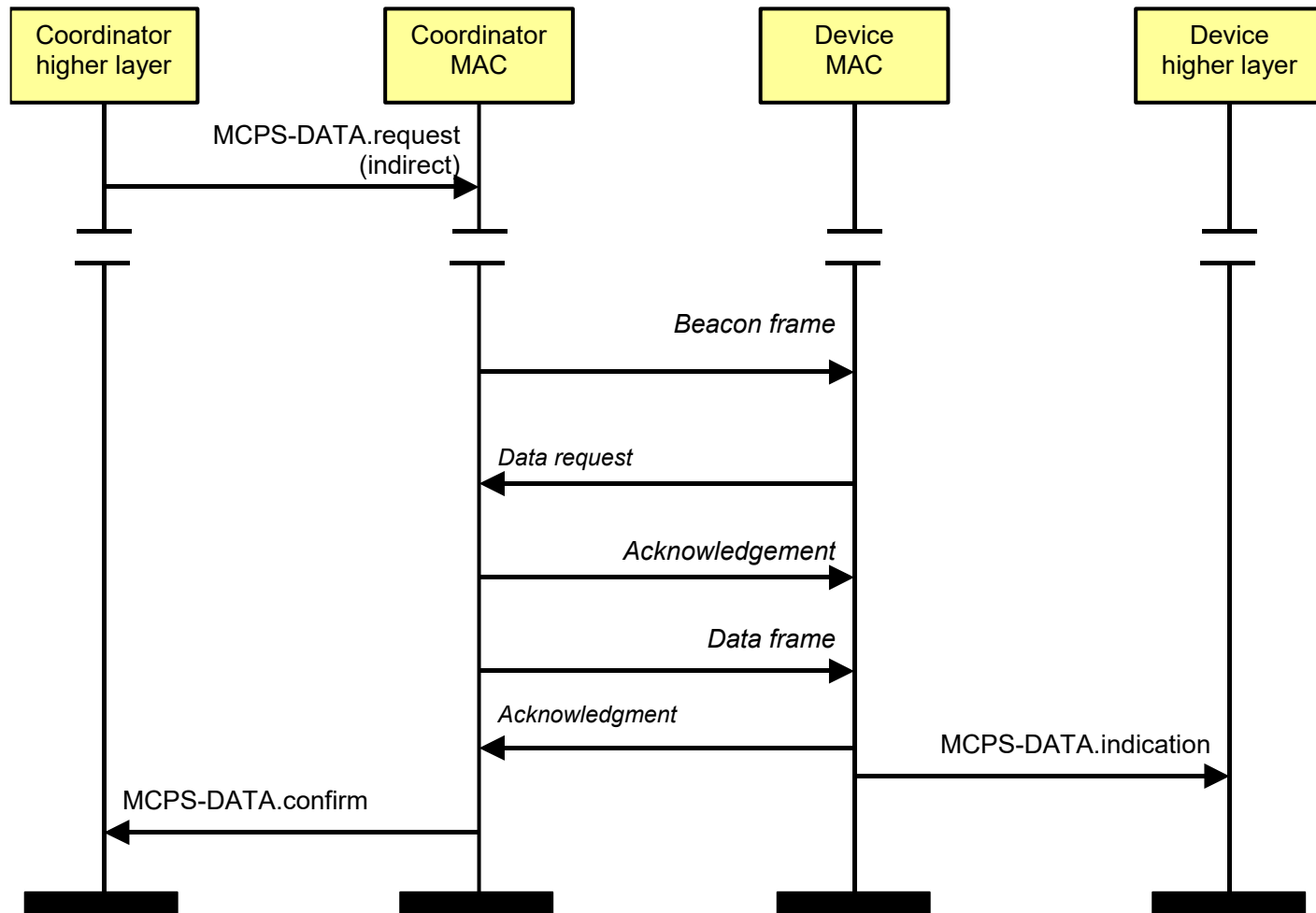


Data Transfer

Message Sequence Diagram



Indirect Data Transfer Message Sequence Diagram



IEEE 802.15.4 MAC: Power

- ▶ Major Source of Energy Waste
- ▶ Consumption occurs in three domains
 - ▶ Sensing
 - ▶ Data processing
 - ▶ Communications
- ▶ Energy Communication waste
 - ▶ Idle listening as dominant factor in most applications
 - ▶ Collision
 - ▶ Overhearing
 - ▶ Control packet overhead



IEEE 802.15.4 MAC: Power

- ▶ 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
 - ▶ Radio-on current is similar for idle listening, RX and TX.
 - ▶ Examples
 - CC2420: RX 18.8 mA, TX 17.4 mA (0 dBm)
 - nRF52840: RX 4.6 mA, TX 4.8 mA (0 dBm)



IEEE 802.15.4 MAC: Power

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



WSN MAC Approaches: Low Power Listening

▶ Channel polling

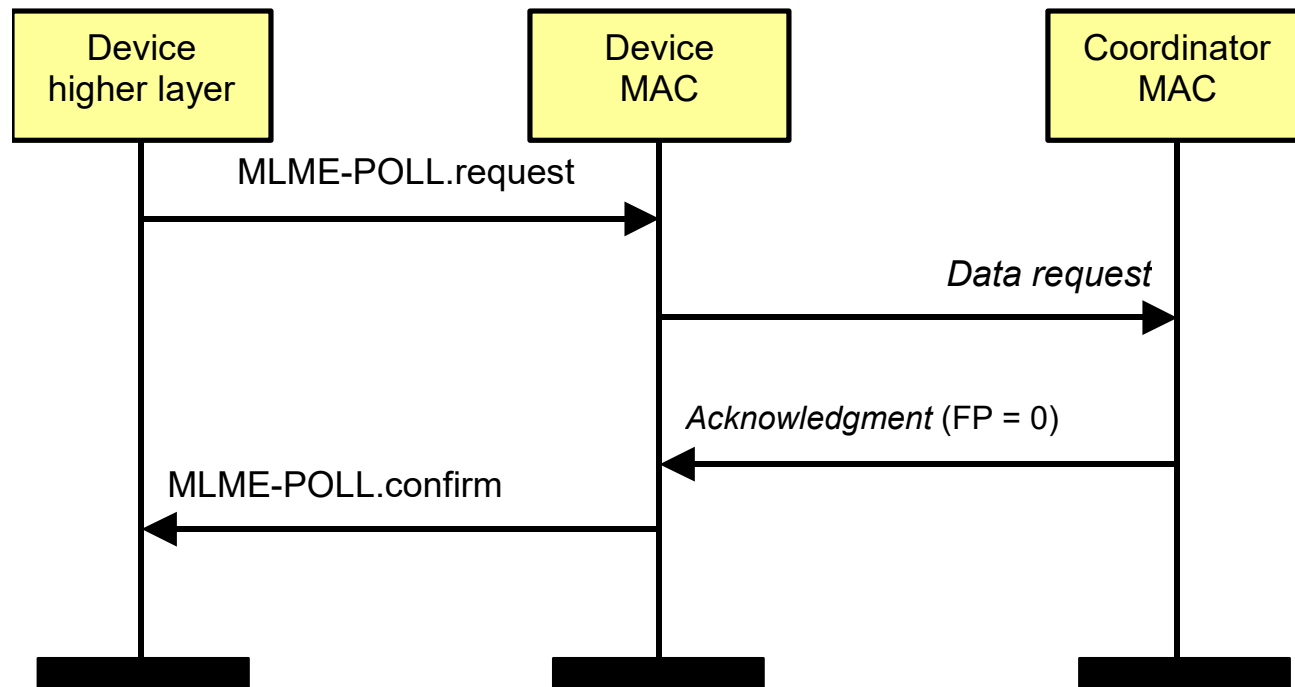
- ▶ Nodes wake up very briefly to check channel activity without receiving data
 - ▶ If channel idle node go back to sleep otherwise it stays awake to receive data
 - ▶ Performed regularly but not synchronised among nodes

▶ Rendezvous with receivers

- ▶ Senders send a long preamble before each message to intersect with a polling
- ▶ Not part of the 802.15.4 standard; CSL (802.15.4e) is the standardized relative



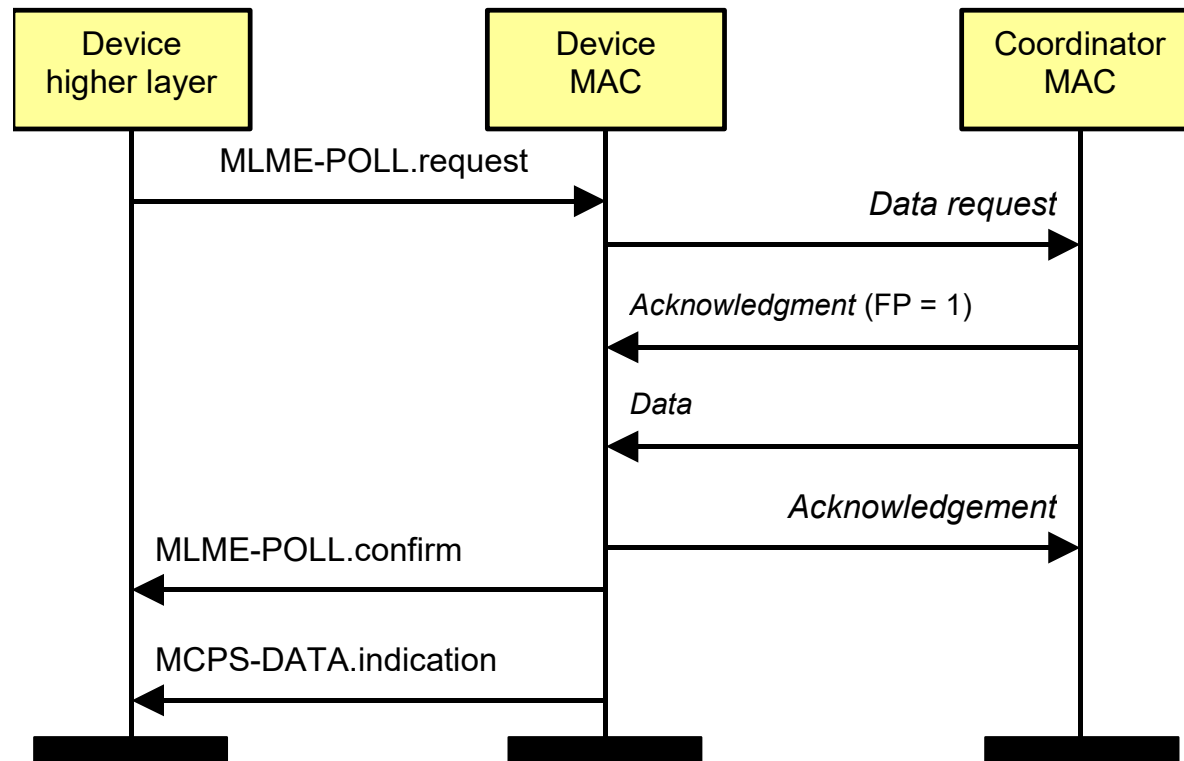
Indirect Polling: No Data Pending Message Sequence Chart



No data pending at the coordinator



Indirect Polling: Data Pending Message Sequence Chart



Data pending at the coordinator



Coordinated Sampled Listening (CSL)

► Challenge:

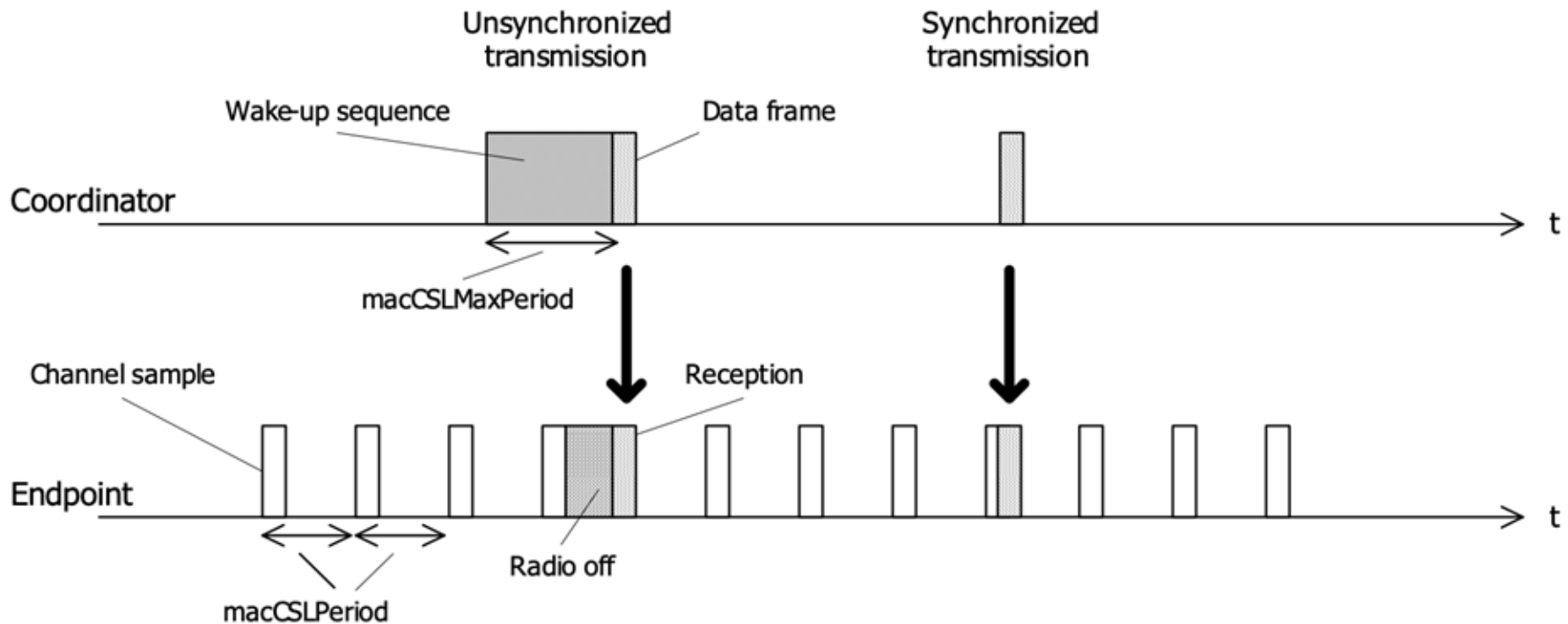
- How does the sender know the receiver is listening?

► Approach:

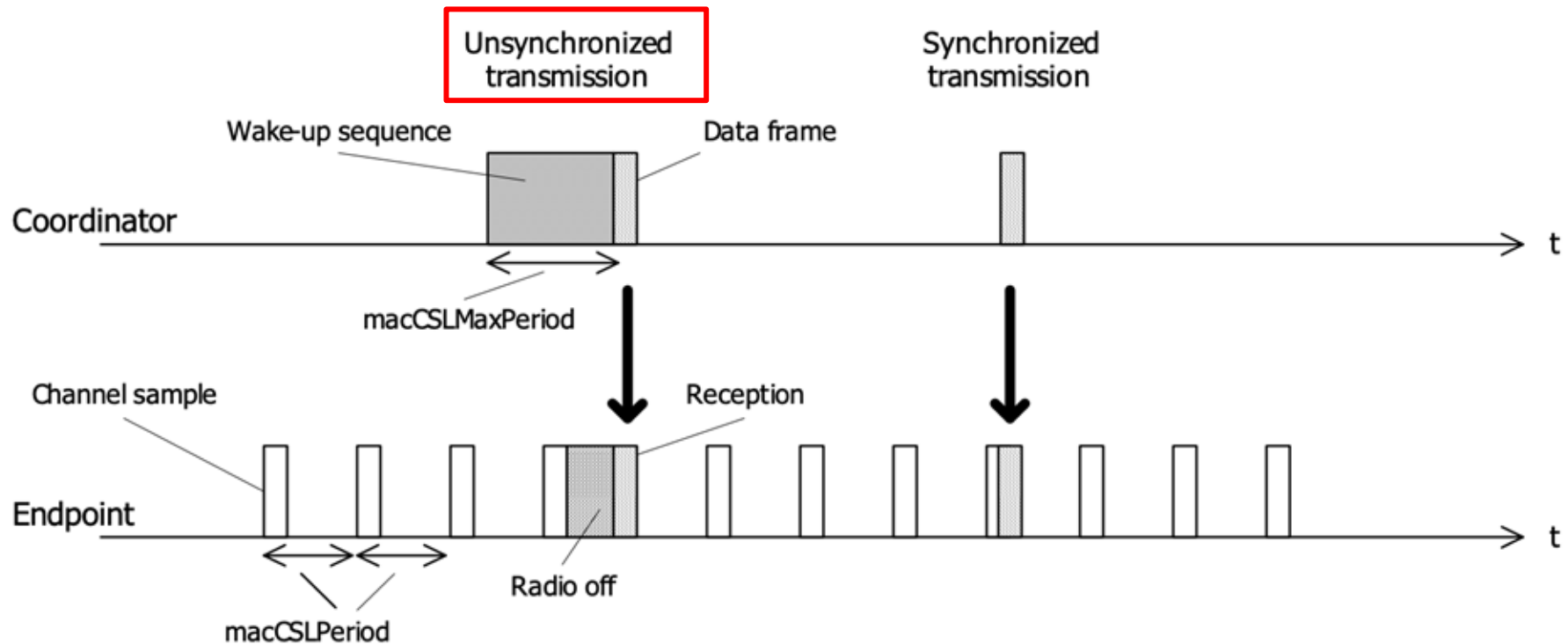
- Start unsynchronized
- Synchronize with wake up-sequence + ack
- Continue data communication at synchronized times
- Defined in IEEE 802.15.4e (2012); part of 802.15.4-2015



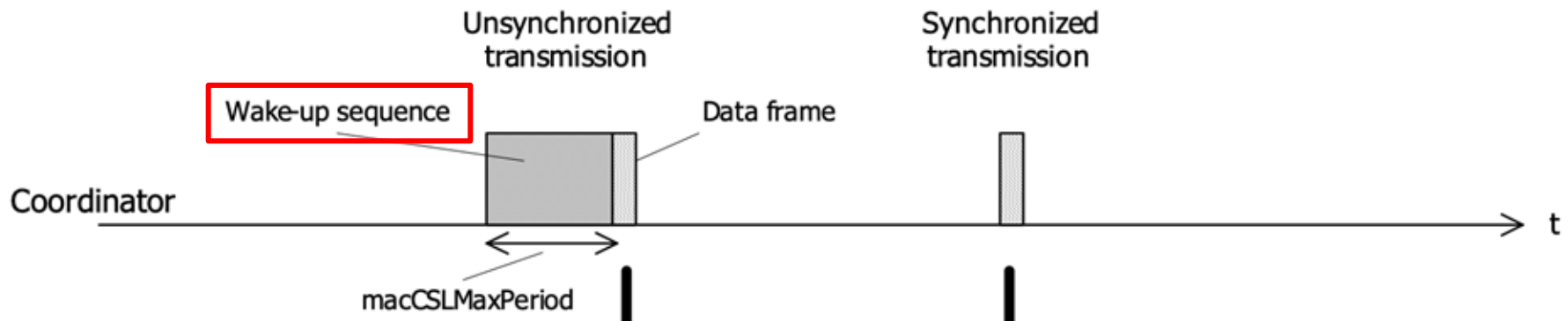
Coordinated Sampled Listening (CSL)



Coordinated Sampled Listening (CSL)

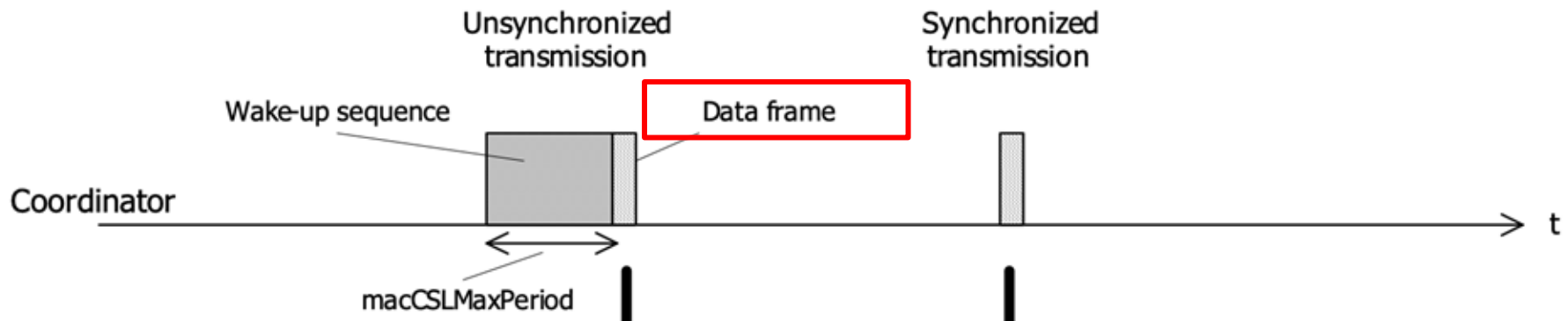


Coordinated Sampled Listening (CSL)



- Coordinator sends a sequence of wake-up frames (wake-up sequence, a train of wake-up frames)

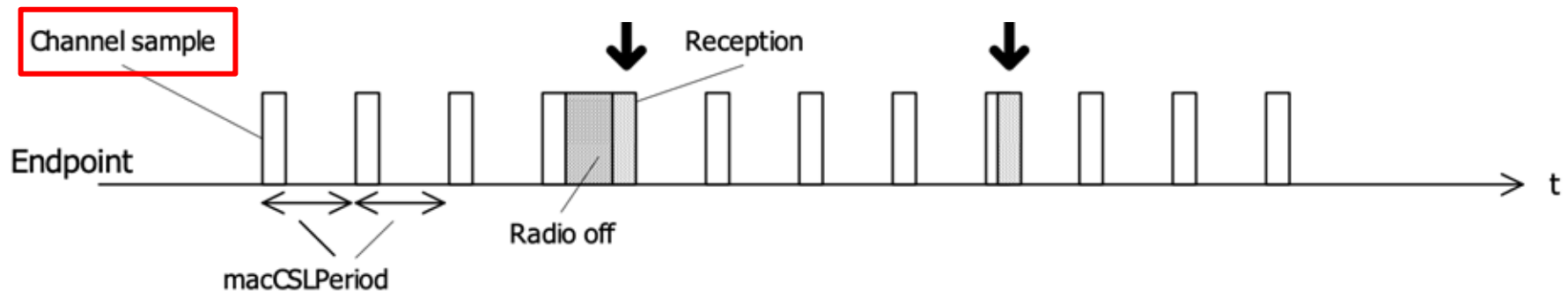
Coordinated Sampled Listening (CSL)



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

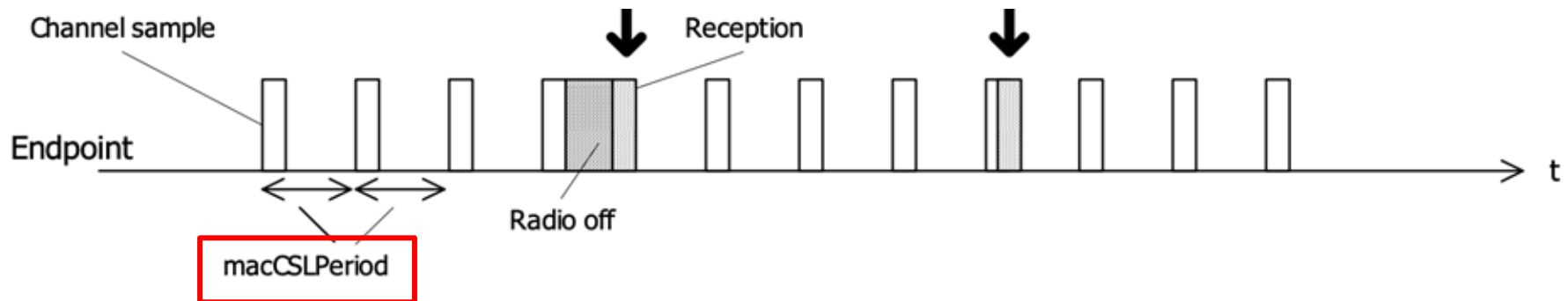
Coordinated Sampled Listening (CSL)

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



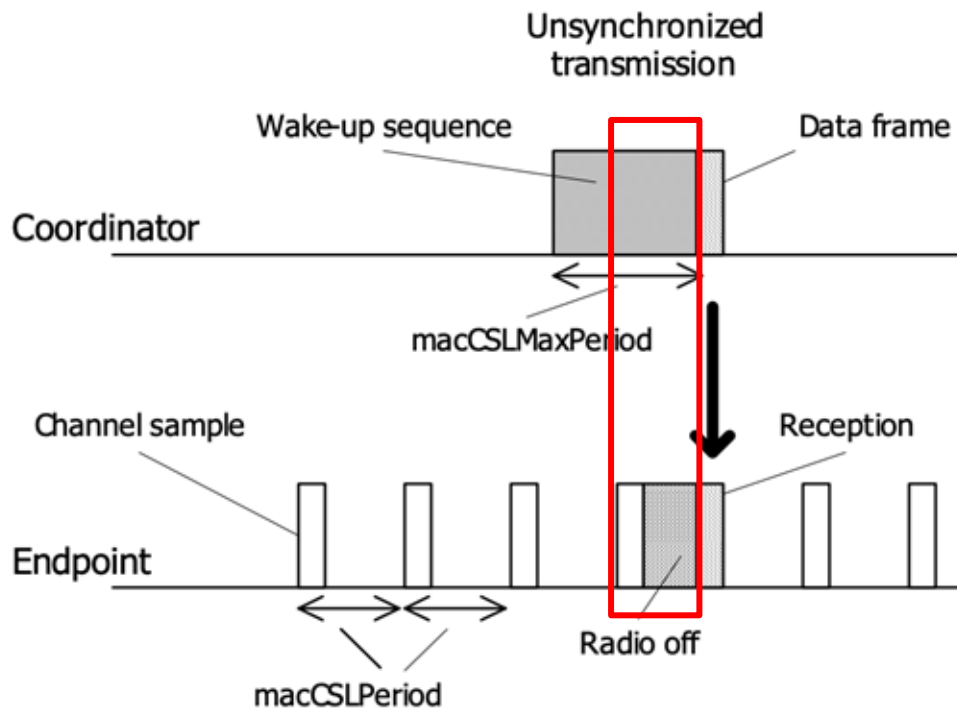
Coordinated Sampled Listening (CSL)

- ▶ 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`



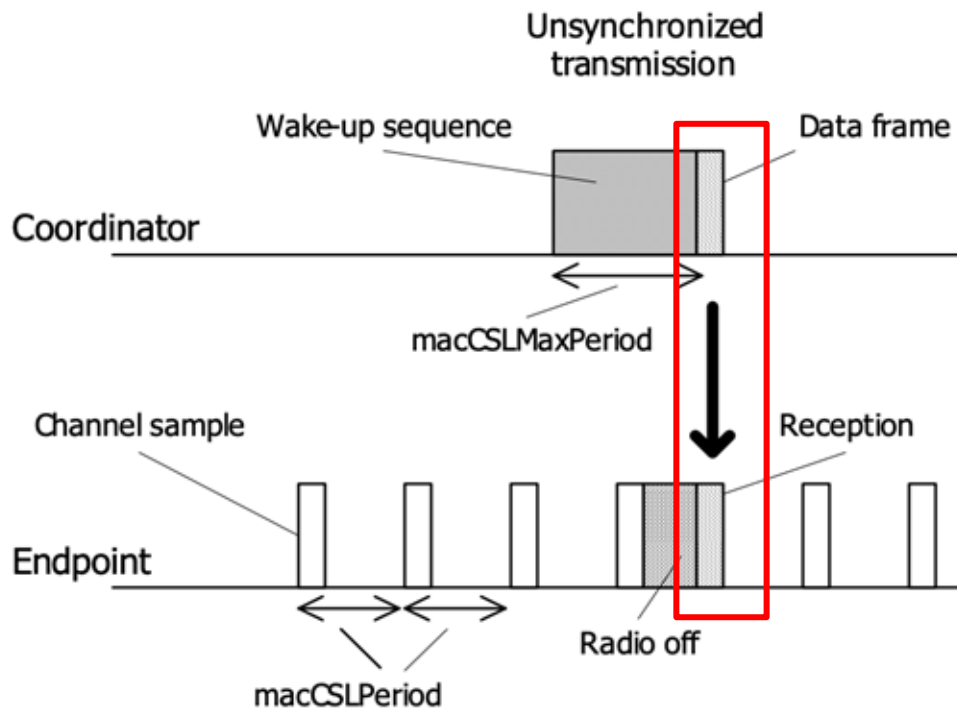
Coordinated Sampled Listening (CSL)

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



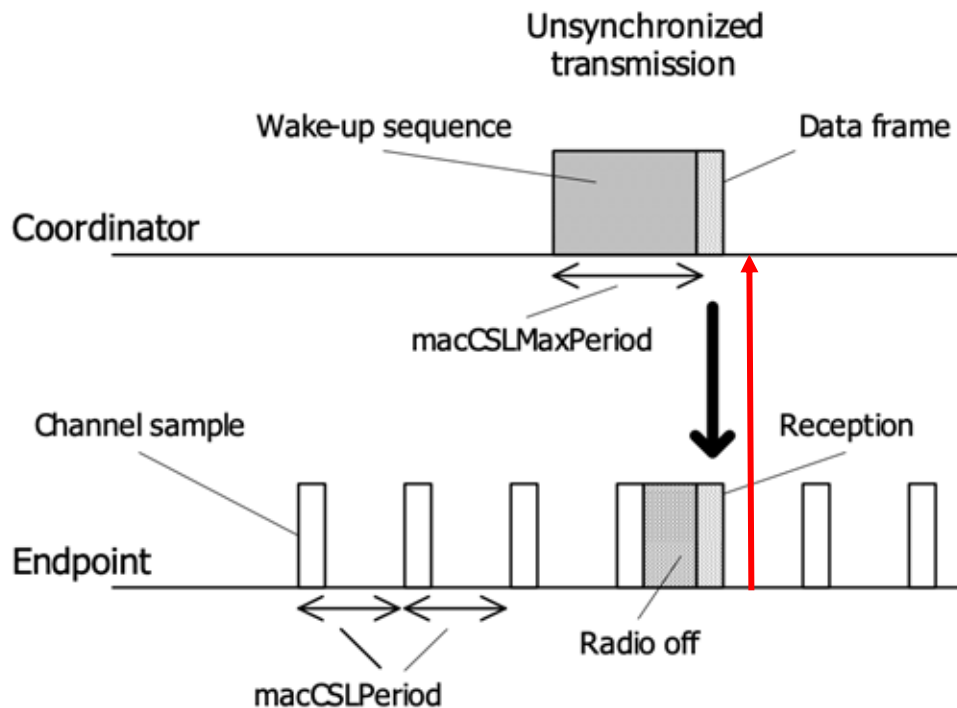
Octets: 2	2
Rendezvous Time	Wake-up Interval

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 Rendezvous time for data
- ▶ Sleeps until Rendezvous time
- ▶ Retrieves data frame at Rendezvous time
- ▶ Ack's back CSL period and CSL Phase

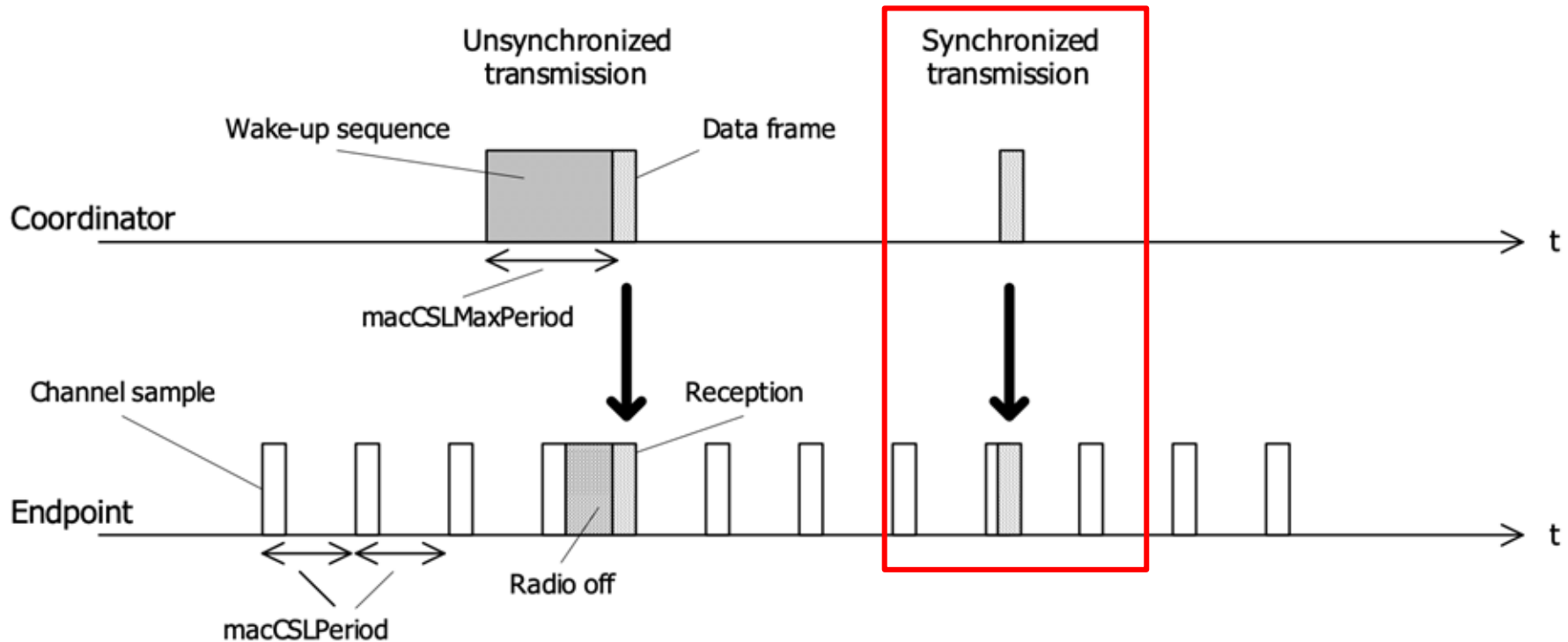
Coordinated Sampled Listening (CSL)

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

- ▶ CSL Phase: time from the end of a frame to the receiver's next channel sample
- ▶ CSL Period: Time between receiver samples



Coordinated Sampled Listening (CSL)



Coordinated Sampled Listening (CSL)

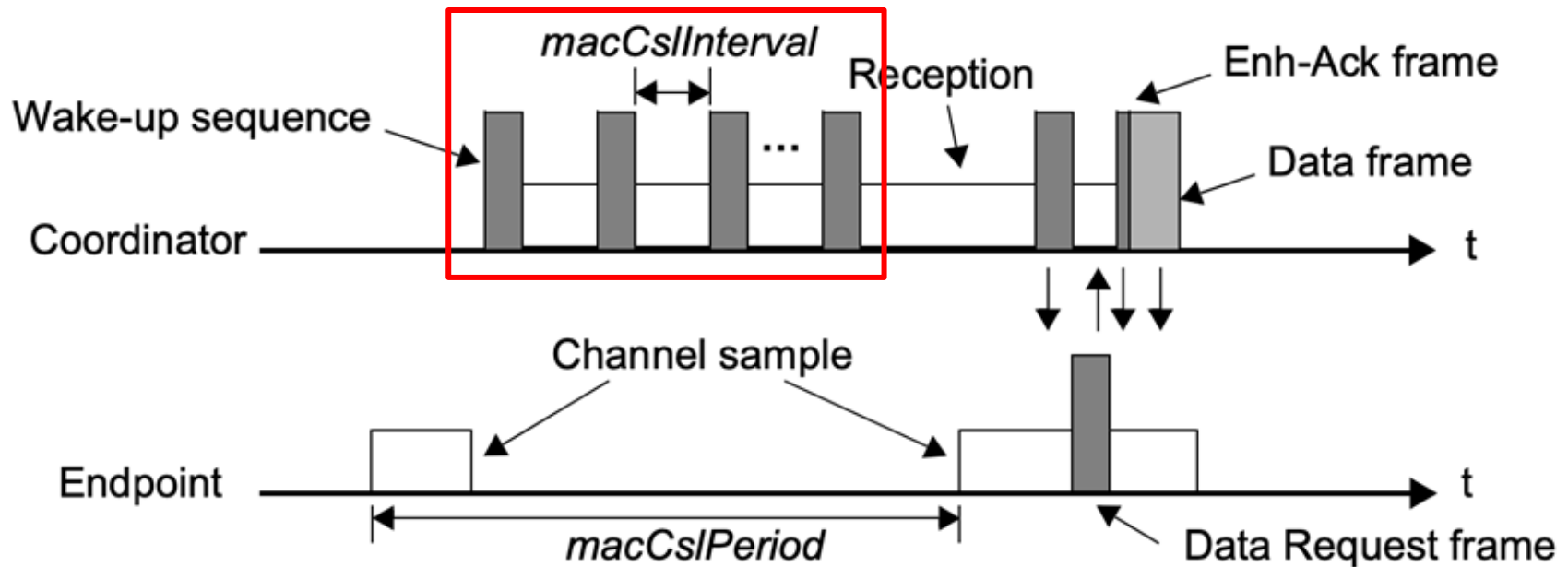
- ▶ What if the wake-up interval (gap between wake-up frames) is nonzero?

Octets: 2	2
Rendezvous Time	Wake-up Interval



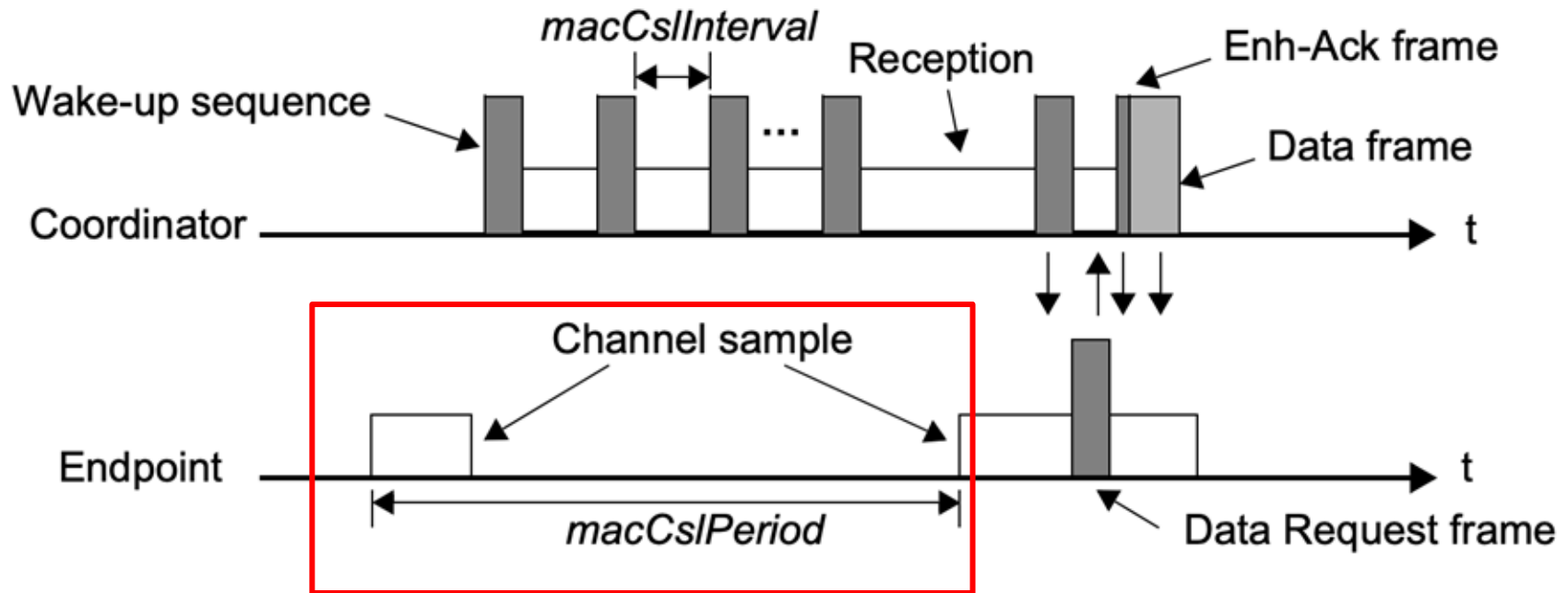
Coordinated Sampled Listening (CSL)

► Wake-up interval nonzero:



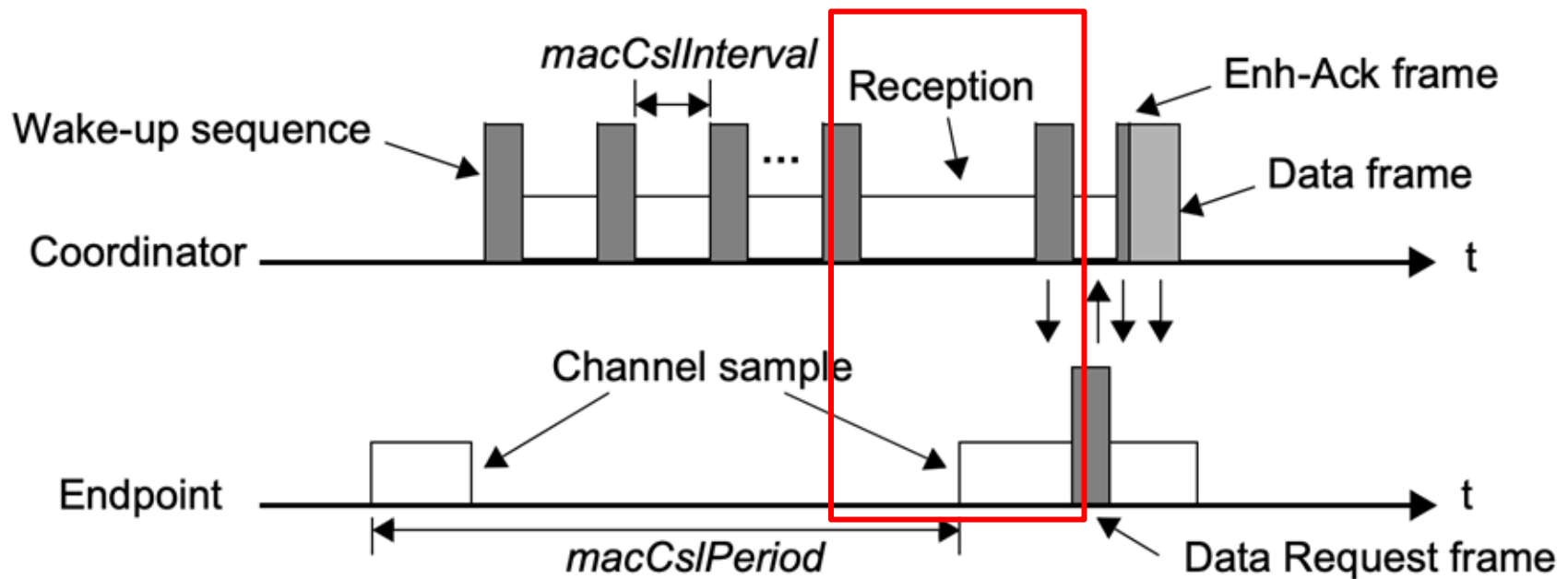
Coordinated Sampled Listening (CSL)

► Wake-up interval nonzero:



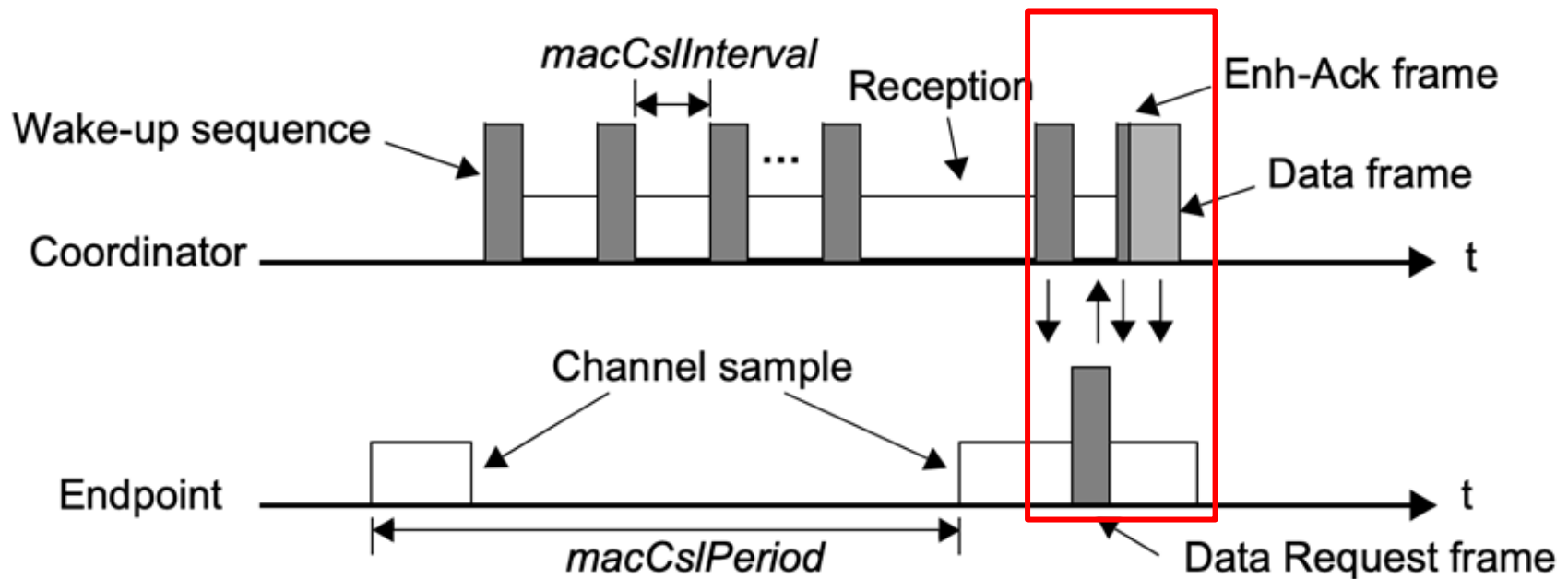
Coordinated Sampled Listening (CSL)

► Wake-up interval nonzero:



Coordinated Sampled Listening (CSL)

► Wake-up interval nonzero:



WSN MAC Approaches: Low Power Listening

► Pros

- Far cheaper than listening for the full contention period (savings depend on poll interval)
- 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



WSN MAC Approaches: 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



IEEE 802.15.4 MAC: Beacon Frame Structure

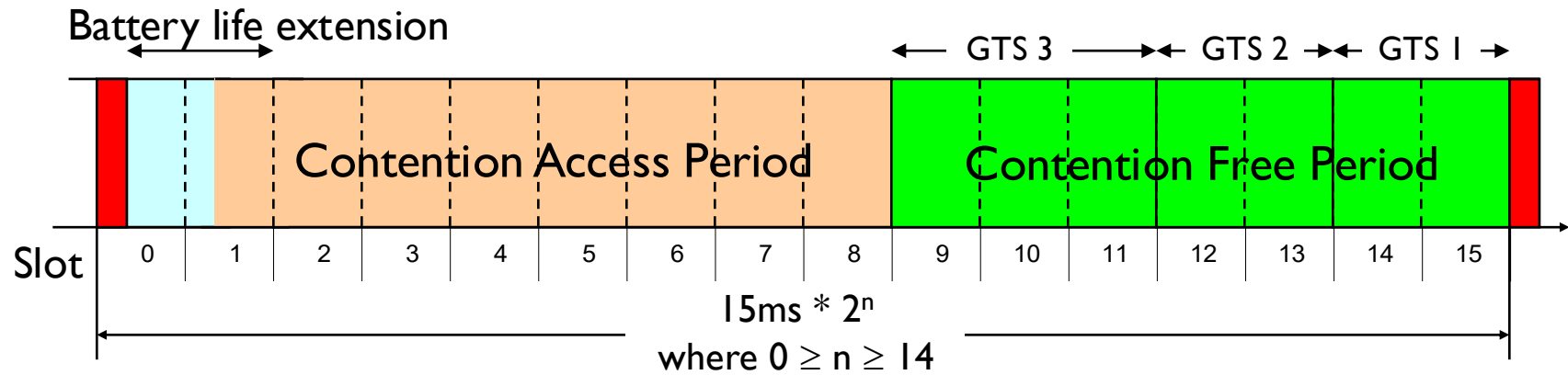
Octets:2	1	4 or 10	2	variable	variable	variable	2
Frame control	Beacon sequence number	Source address information	Superframe specification	GTS fields	Pending address fields	Beacon payload	Frame check sequence
MAC header			MAC payload				MAC footer

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

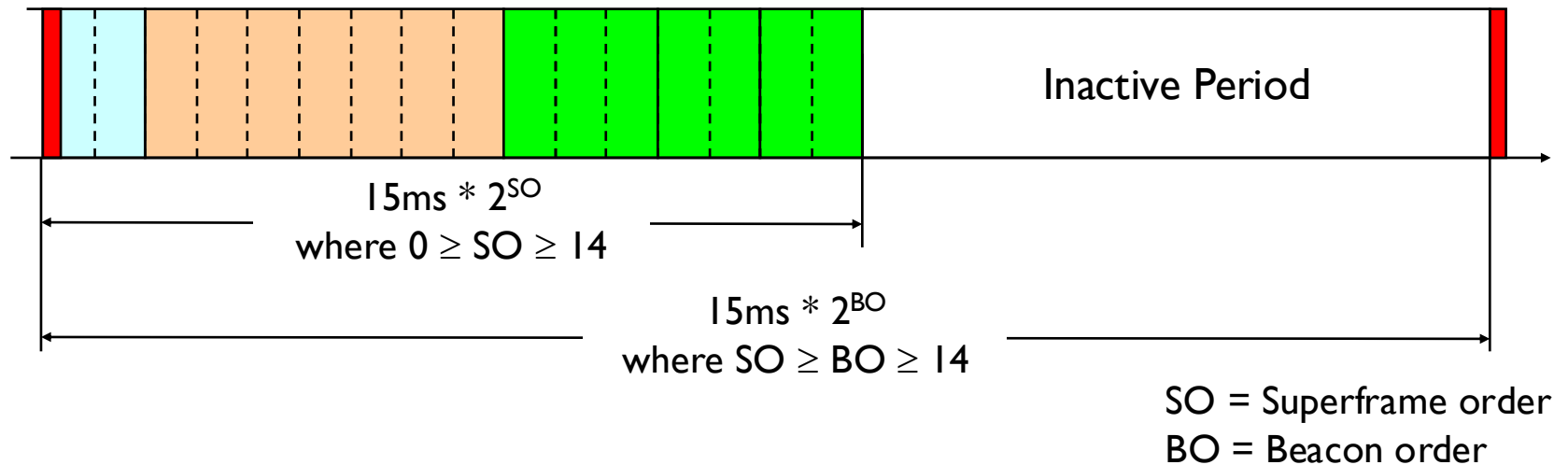


IEEE 802.15.4 MAC: Optional Superframe Structure



- | | | |
|-------------------------|---|--|
| 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

- $\text{BI} = 15.36 \text{ ms} \times 2^{\text{BO}}$; $\text{SD} = 15.36 \text{ ms} \times 2^{\text{SO}}$ (2.4 GHz, $0 \leq \text{SO} \leq \text{BO} \leq 14$)

WSN MAC Approaches: 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



WSN MAC Approaches: 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



WSN MAC Approaches: 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



TSCH: Time-Slotted Channel Hopping

- ▶ IEEE 802.15.4e
 - ▶ Time slots, a repeating slotframe, and channel hopping
 - ▶ A slot is long enough for one frame and its ACK
 - ▶ The schedule tells each node, per slot
 - ▶ Transmit, receive, or sleep, and on which channel offset
 - ▶ Channel changes every slot
 - ▶ $\text{Channel} = \text{table}[(\text{slot number} + \text{offset}) \bmod \text{channels}]$
- ▶ Benefits
 - ▶ No collisions on dedicated slots
 - ▶ Hopping avoids narrowband interference and multipath fades
 - ▶ Radios sleep between slots
- ▶ Nodes stay synchronized using ACK timing and enhanced beacons
- ▶ 6TiSCH runs IPv6 (6LoWPAN) over TSCH for industrial meshes



From 802.15.4 to Zigbee

▶ Zigbee

▶ Network layer (NWK)

- ▶ Turns peer-to-peer links into a self-healing mesh

▶ Application Support + Zigbee Device Objects

- ▶ Lets devices from different vendors interoperate

▶ Security

- ▶ Network-wide and device-to-device key management

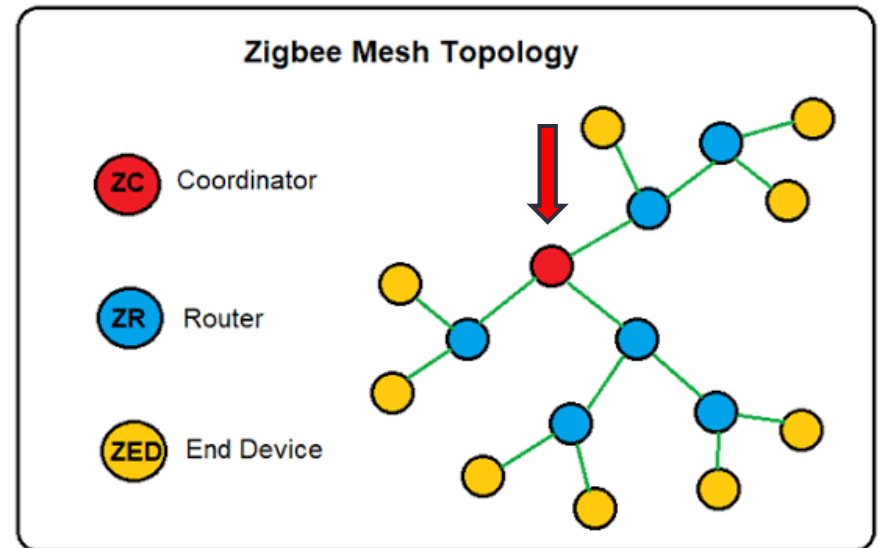
▶ Result

- ▶ Zigbee coordinator, routers, and end devices can form a network that spans far beyond any single radio's range



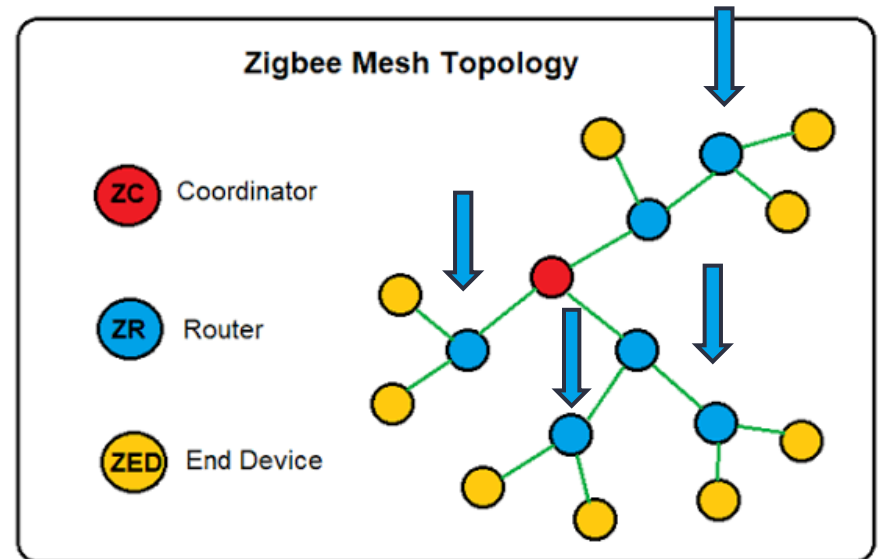
Zigbee Device Roles

- ▶ **Coordinator (ZC)**
 - ▶ Exactly one per network
 - ▶ Starts the PAN
 - ▶ Selects channel
 - ▶ Selects PAN ID
 - ▶ Usually also the Trust Center (holds and distributes security keys)



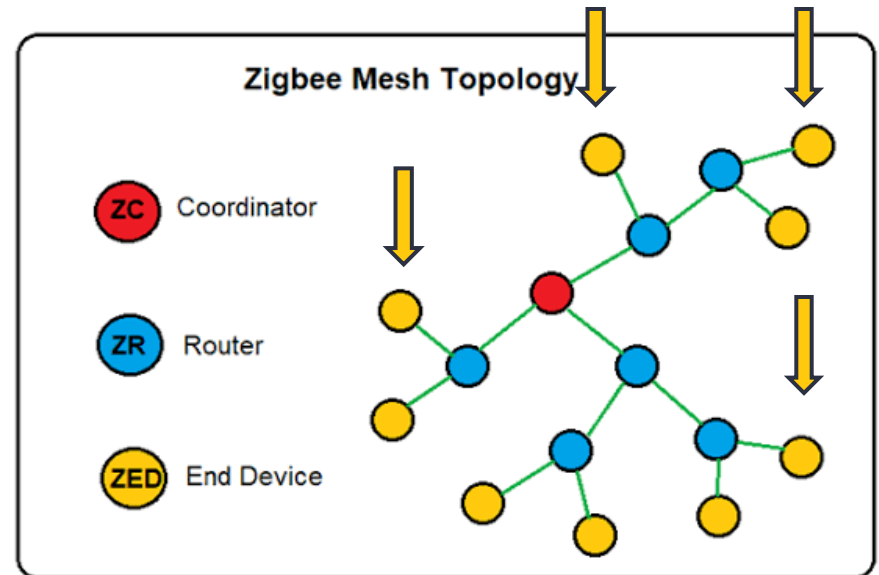
Zigbee Device Roles

- ▶ **Router (ZR)**
 - ▶ Full Function Device
 - ▶ Joins an existing network and relays messages for others
 - ▶ Extends range and provides alternate paths through the mesh



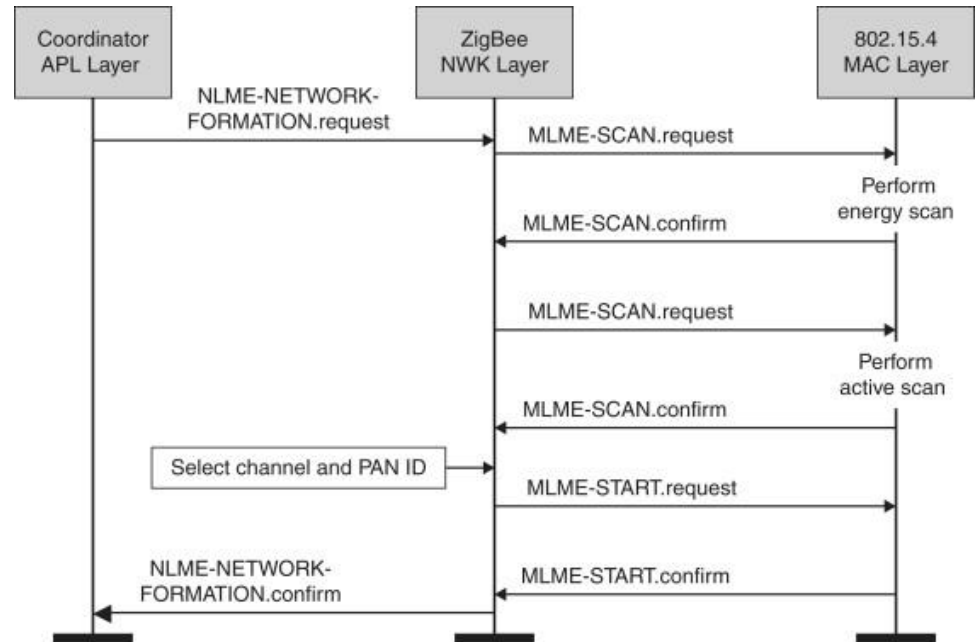
Zigbee Device Roles

- ▶ **End Device (ZED)**
 - ▶ Talks only through its parent Router or Coordinator
 - ▶ Usually battery-powered devices



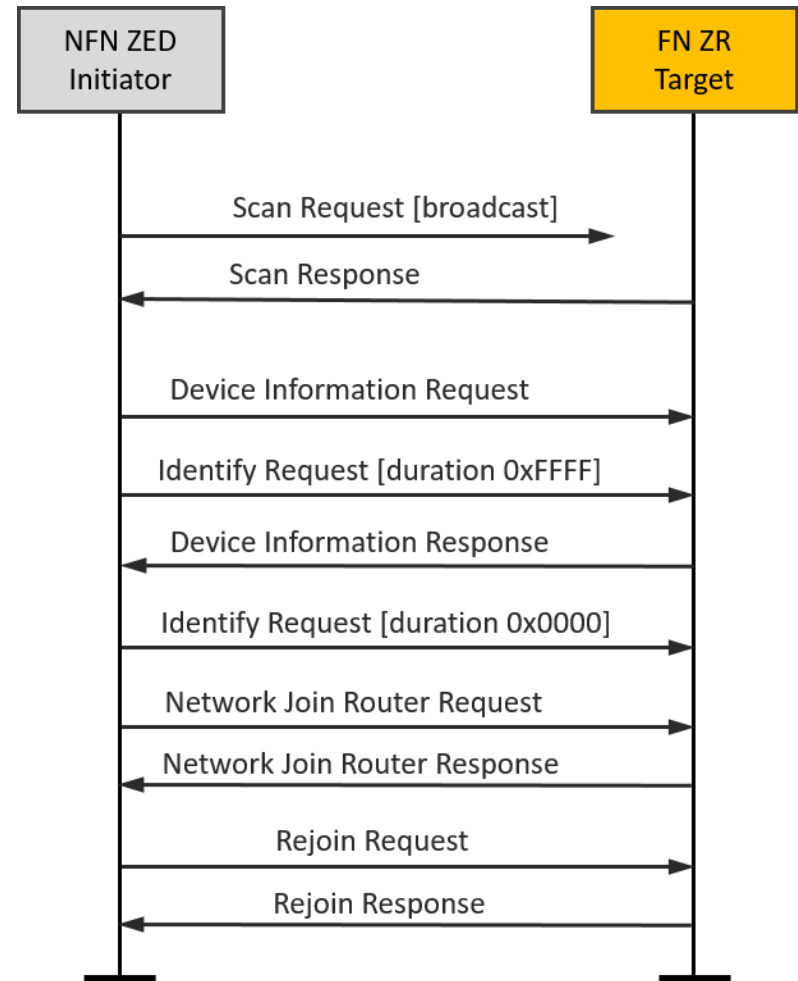
Zigbee Network Formation

- ▶ **Coordinator**
 - ▶ Performs an energy/active scan
 - ▶ Picks a clear channel and PAN ID
 - ▶ Starts the network



Zigbee Network Formation

- ▶ Routers and End Devices
 - ▶ Discover the coordinator via passive/active scan, then associate



Zigbee Network Addressing

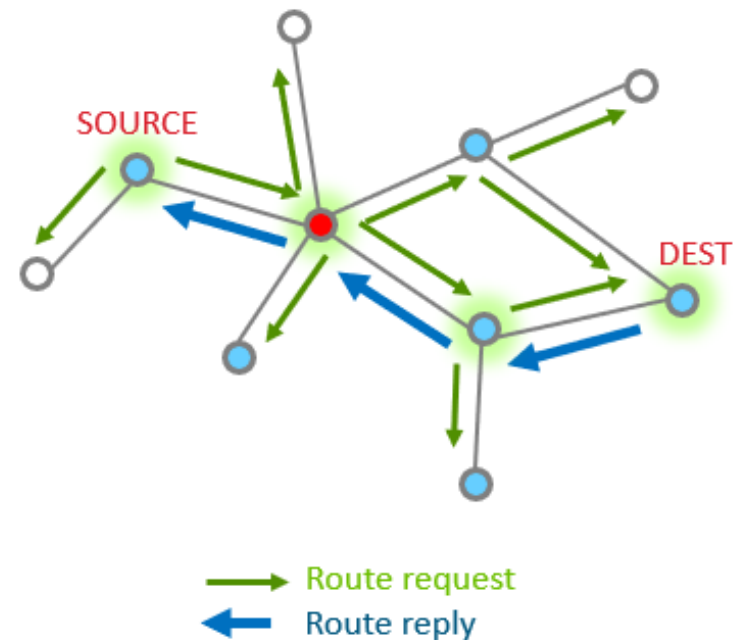
▶ Addressing

- ▶ Every device keeps its 64-bit IEEE address
- ▶ Also assigned a short 16-bit network address for routing
- ▶ Early Zigbee versions assigned these addresses via a distributed tree formula
- ▶ Modern Zigbee uses random assignment with conflict detection



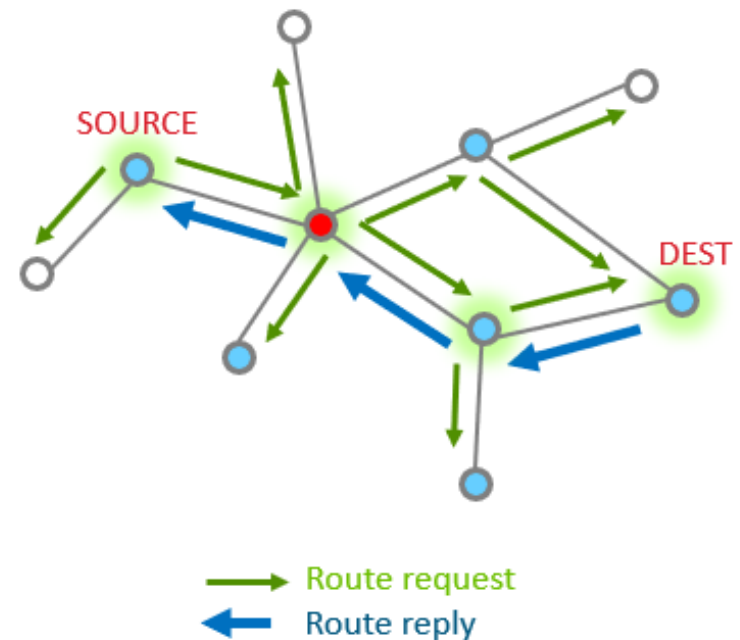
Zigbee Mesh Routing

- ▶ Zigbee PRO uses AODV-style routing (Ad-hoc On-Demand Distance Vector)
 - ▶ A Router with no known route floods a Route Request
 - ▶ The destination (or a Router that knows a route) replies
 - ▶ Routers cache the discovered route in a routing table for reuse



Zigbee Mesh Routing

- ▶ **Many-to-One routing**
 - ▶ Common case: many devices all report back to one collector (e.g., the Coordinator)
 - ▶ One route discovery lets every node learn a route to that one destination, instead of running separate discoveries
 - ▶ Return path: the collector uses source routes built from the route records each node sends
- ▶ **Self-healing**
 - ▶ If a Router fails, neighboring nodes lose their route through it and simply discover a new one



6LoWPAN: IPv6 on 802.15.4

▶ Problem

- ▶ IPv6 expects 1280-byte packets
- ▶ an 802.15.4 frame carries at most 127 bytes
- ▶ After MAC header and security, about 80 bytes remain for upper layers

▶ 6LoWPAN adapts IPv6 to small, low-power links

▶ Header compression

- ▶ 40-byte IPv6 header can shrink to a few bytes
- ▶ Uses link-layer addresses and shared context instead of sending them again

▶ UDP header compression

- ▶ 8 bytes can shrink to as few as 4

▶ Fragmentation and reassembly for larger packets

▶ Result: every sensor can be a normal IPv6 host

- ▶ Defined in RFC 4944 and RFC 6282



Thread: Another Mesh Built on 802.15.4

- ▶ **On top of IEEE 802.15.4 PHY/MAC**
 - ▶ Different network layer than ZigBee
- ▶ **Thread is IPv6-native**
 - ▶ Uses 6LoWPAN to compress full IPv6 packets onto 802.15.4 frames
 - ▶ No separate Zigbee-style NWK addressing scheme
 - ▶ Every device is a real IPv6 host



Thread: Another Mesh Built on 802.15.4

▶ Device roles

▶ Leader

- ▶ Elected, one per network partition
- ▶ Assigns router addresses

▶ Router / REED (Router-Eligible End Device)

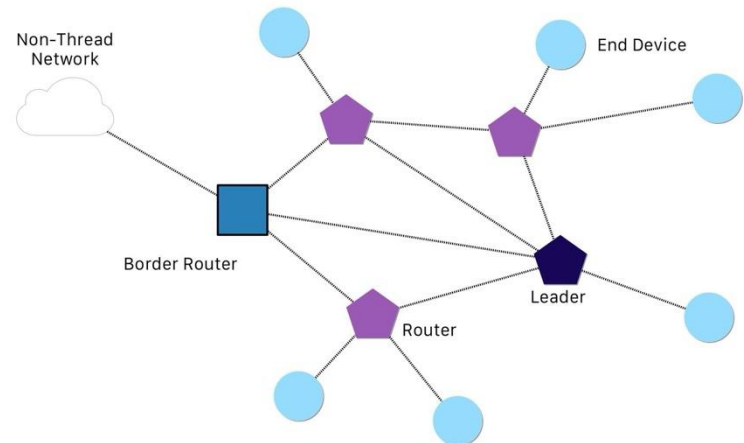
- ▶ Can relay traffic; REEDs are promoted to Router when the network has fewer than 16 routers (limit: 32)

▶ End Device

- ▶ Talks only through a parent Router

▶ Border Router

- ▶ Bridges the Thread mesh to Wi-Fi/Ethernet and the internet



Thread: How the Mesh Operates

- ▶ Routers form the backbone (up to 32 per network)
 - ▶ One is elected Leader
- ▶ MLE (Mesh Link Establishment) sets up links and shares route costs
- ▶ Routing is plain IPv6, done by Thread routers (route-over)
- ▶ Sleepy end devices poll their parent
 - ▶ Parent buffers messages until the child polls (like the indirect transfer earlier)
 - ▶ Poll period sets the latency / battery trade-off
- ▶ Border Router connects the mesh to Wi-Fi/Ethernet
 - ▶ Devices get a mesh-local address plus a global IPv6 address
- ▶ Security
 - ▶ AES-128 at the MAC layer with a network key



Thread: Partitions and Commissioning

- ▶ **Partitions:** if the mesh splits, each side elects its own Leader
 - ▶ When the halves reconnect, the partitions merge and one Leader remains
- ▶ **Commissioning a new device**
 - ▶ A commissioner (phone app or border router) authenticates the joiner with its joining credential, e.g., a QR code
 - ▶ It then delivers the network credentials (name, key, channel, PAN ID)
 - ▶ The joiner attaches to a parent router as a child
- ▶ **Router count:** promote REEDs below 16 routers; limit of 32



Routing and Resilience

Zigbee

- ▶ **Routing**
 - ▶ On-demand (AODV)
 - ▶ Floods a Route Request only when a route is needed
- ▶ **Single point of failure**
 - ▶ One Trust Center (usually the Coordinator) issues all keys
- ▶ **Addressing**
 - ▶ Proprietary 16-bit network address, translated by the NWK layer

Thread

- ▶ **Routing**
 - ▶ Proactive distance-vector
 - ▶ Routers continuously exchange path costs (via MLE), so a route is already known before it's needed
- ▶ **Single point of failure**
 - ▶ Leader role re-elects automatically if the current Leader drops off
 - ▶ No fixed anchor device
- ▶ **Addressing**
 - ▶ Standard IPv6 addresses throughout
 - ▶ Talks directly to other IP devices via its Border Router



Zigbee Application Layer

- ▶ **Application Support Sub-layer (APS)**
 - ▶ Sits between NWK and the application
 - ▶ Handles bindings (device-to-device links) and end-to-end security
- ▶ **Zigbee Device Objects (ZDO)**
 - ▶ Handles device/service discovery, network management, and how devices join/leave
- ▶ **Clusters and attributes**
 - ▶ Applications are built from standardized clusters
 - ▶ e.g., 'On/Off', 'Temperature Measurement', 'Level Control'
 - ▶ A switch and a bulb from different manufacturers interoperate because both implement the same cluster



Zigbee Application Model

- ▶ **Endpoint**
 - ▶ One application on a device
 - ▶ Numbered 1–240; endpoint 0 is ZDO
- ▶ **Cluster**
 - ▶ Related attributes and commands, defined in the Zigbee Cluster Library (ZCL)
 - ▶ Attribute = state (OnOff = true); command = action (Toggle)
- ▶ **Binding**
 - ▶ Table entry linking a source endpoint and cluster to a destination
 - ▶ A switch sends commands to its bulb without knowing its address
- ▶ **Group**
 - ▶ One command reaches many devices
- ▶ **Example**
 - ▶ Press switch, On/Off Toggle command goes via the binding to the bulb, its OnOff attribute flips and is reported back



Joining a Zigbee Network

1. A router or the coordinator opens a joining window and advertises it in beacons
 2. The new device scans, picks a parent, and associates
 3. The Trust Center sends the network key, encrypted with a link key
 4. The device announces itself; the Trust Center may require a new unique link key
- ▶ Which link key protects step 3?
 - ▶ Global default key (ZigBeeAlliance09): the same for every device, so a sniffer that captures a join learns the network key
 - ▶ Install code: a unique per-device code (16 bytes + CRC), hashed into a unique key
 - ▶ Zigbee 4.0 adds dynamic link keys and a device interview step



Zigbee 3.0: Unifying the Ecosystem (2016)

▶ Pre 3.0

- ▶ Separate, incompatible application profiles
- ▶ Home Automation, Light Link, Smart Energy, etc
- ▶ A Light Link bulb couldn't talk to a Home Automation switch

▶ Zigbee 3.0 provides one certifiable standard

- ▶ Base Device Behavior specification
 - ▶ Common rules for joining, discovery, and security
- ▶ Any Zigbee 3.0 certified device is expected to interoperate with any other, regardless of vendor



Green Power: Batteryless Zigbee Devices

▶ Green Power (ZGP)

- ▶ Supports energy-harvesting devices with no battery
 - ▶ E.g.: kinetic (push-button-powered) light switches, solar-powered sensors
- ▶ Can't run a full Zigbee stack or stay awake to route
 - ▶ A nearby powered Router acts as a Green Power Proxy, handling the network-side
 - ▶ Communication is simplified and mostly one-way to keep energy cost near zero



Commissioning: Touchlink and Green Power

- ▶ **Touchlink: commissioning by proximity**
 - ▶ The remote or phone must be very close to the lamp (strong signal)
 - ▶ Adds or resets lights without a coordinator
- ▶ **Green Power pairing**
 - ▶ Press the device's commissioning button: it sends a commissioning frame
 - ▶ A Green Power Proxy (any mains-powered router) forwards it
 - ▶ A Green Power Sink (lamp or hub) stores the device ID and security key
- ▶ **Afterwards each button press is one small frame with a counter**
 - ▶ Proxies forward it; sinks check the counter to reject replays



Matter: One Application Layer

- ▶ **Matter (CSA, 1.0 in 2022)**
 - ▶ Common smart-home application layer
 - ▶ Runs over IP (IPv6, UDP), on Wi-Fi, Ethernet, or Thread
 - ▶ BLE is used only to commission new devices
- ▶ **Goal**
 - ▶ Any Matter device works with any Matter ecosystem
 - ▶ Local control: works without the cloud
- ▶ **Data model**
 - ▶ Nodes, endpoints, clusters (borrowed from Zigbee's cluster ideas)
 - ▶ Read, write, subscribe, and invoke commands
- ▶ **Matter is not a radio or a mesh; Thread supplies the low-power mesh**
 - ▶ Zigbee devices reach Matter through bridges



Matter: Commissioning and Fabrics

- ▶ **Commissioning: adding a device to a home**
 - ▶ Scan the QR code or enter the setup code
 - ▶ Phone and device set up a secure session, often over BLE
 - ▶ Device proves it is certified (device attestation)
 - ▶ Phone gives it a fabric credential plus Wi-Fi or Thread network credentials
 - ▶ Device joins the Wi-Fi or Thread network and is controlled over IP
- ▶ **Multi-admin: one device can belong to several fabrics**
 - ▶ Apple, Google, Amazon, Samsung can all control the same bulb
- ▶ **Thread devices also need a Thread Border Router**



The Stack: 802.15.4 to Zigbee, Thread, and Matter

Layer	Zigbee	Thread + Matter
Application	ZCL clusters (APS, ZDO)	Matter data model (clusters over UDP)
Security	Network key and link keys (AES-CCM*)	Thread network key; Matter certificates (CASE)
Network	Zigbee NWK, AODV-style routing	IPv6 + 6LoWPAN, MLE routing
MAC / PHY	IEEE 802.15.4	IEEE 802.15.4



Zigbee Today

- ▶ ZigBee Alliance renamed Connectivity Standards Alliance (CSA) in 2021
 - ▶ Broader mission
 - ▶ CSA now oversees Zigbee, Matter, and other IoT standards
 - ▶ Matter (2022) is CSA's newer smart-home standard, runs over IP (Wi-Fi, Ethernet, Thread); BLE only for commissioning; not built on Zigbee
 - Ecosystem interoperability (Apple, Google, Amazon, Samsung, etc. all support it)
- ▶ Zigbee remains massively deployed
 - ▶ CSA reports more than 1 billion Zigbee devices deployed (Nov 2025)
 - ▶ Zigbee devices reach Matter ecosystems today through bridges (e.g., Amazon, Google, SmartThings hubs)



Zigbee Direct

- ▶ **Goal**
 - ▶ Add and control Zigbee devices from a phone over BLE
 - ▶ No hub, and no Zigbee radio in the phone
- ▶ A Zigbee Direct-capable device has a BLE interface next to its Zigbee radio
 - ▶ It bridges between the two
- ▶ The phone connects over BLE and its commands are tunneled into the Zigbee network
- ▶ Part of Zigbee 4.0 (Zigbee Direct v1.1 specification)



Zigbee 4.0 (Released November 2025)

- ▶ Fully backward compatible with Zigbee 3.0 and Smart Energy
- ▶ Security overhaul
 - ▶ Dynamic Link Key, Device Interview, Advanced Frame Counter Synchronization (blocks replay attacks)
 - ▶ Restricted Mode, Secured Channel, Trust Center Swap Out for safer network management
- ▶ Easier onboarding
 - ▶ Zigbee Direct
 - ▶ Commission and control devices via Bluetooth Low Energy
 - ▶ No hub required
 - ▶ Batch Commissioning: set up many devices at once
- ▶ Sleeping-to-sleeping device communication
 - ▶ Coordinated Sample Listening (CSL)
 - ▶ Used device-to-device, not just to a coordinator



Suzi: Zigbee's New Sub-GHz Mesh Brand

- ▶ **Suzi = Zigbee's long-range, Sub-GHz mesh networking**
 - ▶ Built directly on the Zigbee network layer
 - ▶ Uses the European 800 MHz and North American 900 MHz PHY bands
- ▶ **Why Sub-GHz?**
 - ▶ Lower frequency → better range and wall penetration than 2.4 GHz
 - ▶ Useful for large properties, outdoor spaces, and building/city-scale deployments
- ▶ **Status: Suzi product certification opened September 2, 2026 (CSA)**



Wi-Fi vs. BLE vs. 802.15.4: Energy and Rate

	Wi-Fi 6 (ESP32-C6)	BLE (nRF52840)	802.15.4 (Zigbee/Thread)
PHY rate	up to 143 Mbps (20 MHz, 1 SS)	1 or 2 Mbps (125–500 kbps coded)	250 kbps (2.4 GHz)
Radio-on power	RX 78 mA = 0.26 W; TX 251 mA = 0.83 W	RX 4.6 mA, TX 4.8 mA $\approx$ 14 mW	$\approx$ 14 mW (nRF52840); CC2420: RX 18.8 mA, TX 17.4 mA
Energy per bit at peak rate (approx.)	$\approx$ 7 nJ/bit (TX, MCS9)	$\approx$ 14 nJ/bit (1M); 7 (2M)	$\approx$ 58 nJ/bit
Topology	Star (AP)	Star; Mesh spec	Mesh (Zigbee, Thread)
Typical use	High throughput	Phones, wearables, audio, tags	Sensors, lighting, Matter over Thread

