Standard IEEE 802.15.4 e Redes ZigBee

José Augusto Afonso
jose.afonso@dei.uminho.pt

IEEE 802.15.4

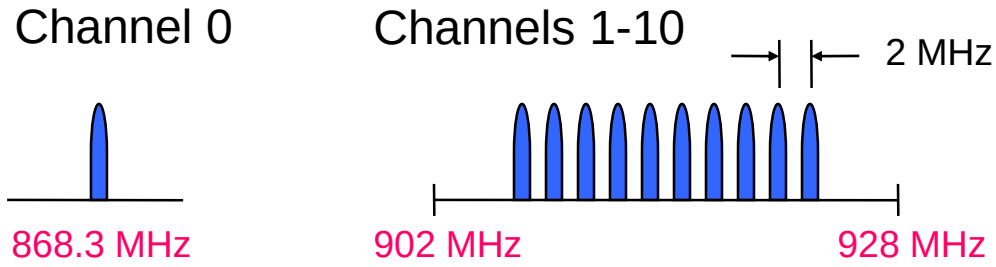
- A standard for wireless sensor networks (PHY and MAC layers)
- Basis of ZigBee, WirelessHART and 6LoWPAN networks
- Data rates up to 250 kbps
- Star or peer-to-peer topologies (other topologies with ZigBee)
- Up to 65535 devices per network
- CSMA/CA channel access, slotted (beacon-enabled) or unslotted
- Support for low-latency devices (beacon-enabled mode, GTS)
- Optional acknowledgement for transfer reliability
- Automatic network establishment by the PAN coordinator
- Dynamic device addressing, flexible addressing format
- Power management to ensure low power consumption
- 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band

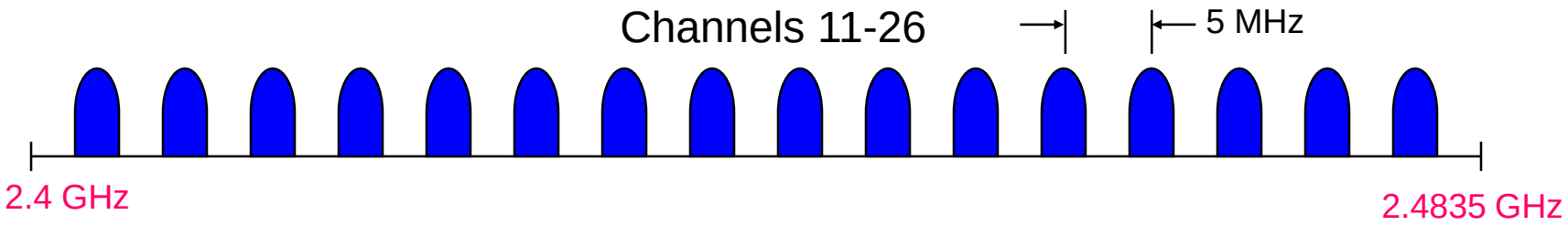
802.15.4 PAN (Personal Area Network)

- Uses a specific 16-bit PAN ID
- A PAN Coordinator "forms" the network
  - Node "0"
  - Chooses radio channel
  - Specifies PAN ID
  - Chooses the security model
  - Starts the network formation process
- Two classes of devices
  - FFD (Full Function Device)
    - Can act as a router
    - Can also perform any other function like sensing
  - RFD (Reduced Function Device)
    - Can't act as a router, only as an end device
    - Can talk only to a FFD
    - Sensors, actuators, etc. that don't need to route data

Frequency Bands and Rates

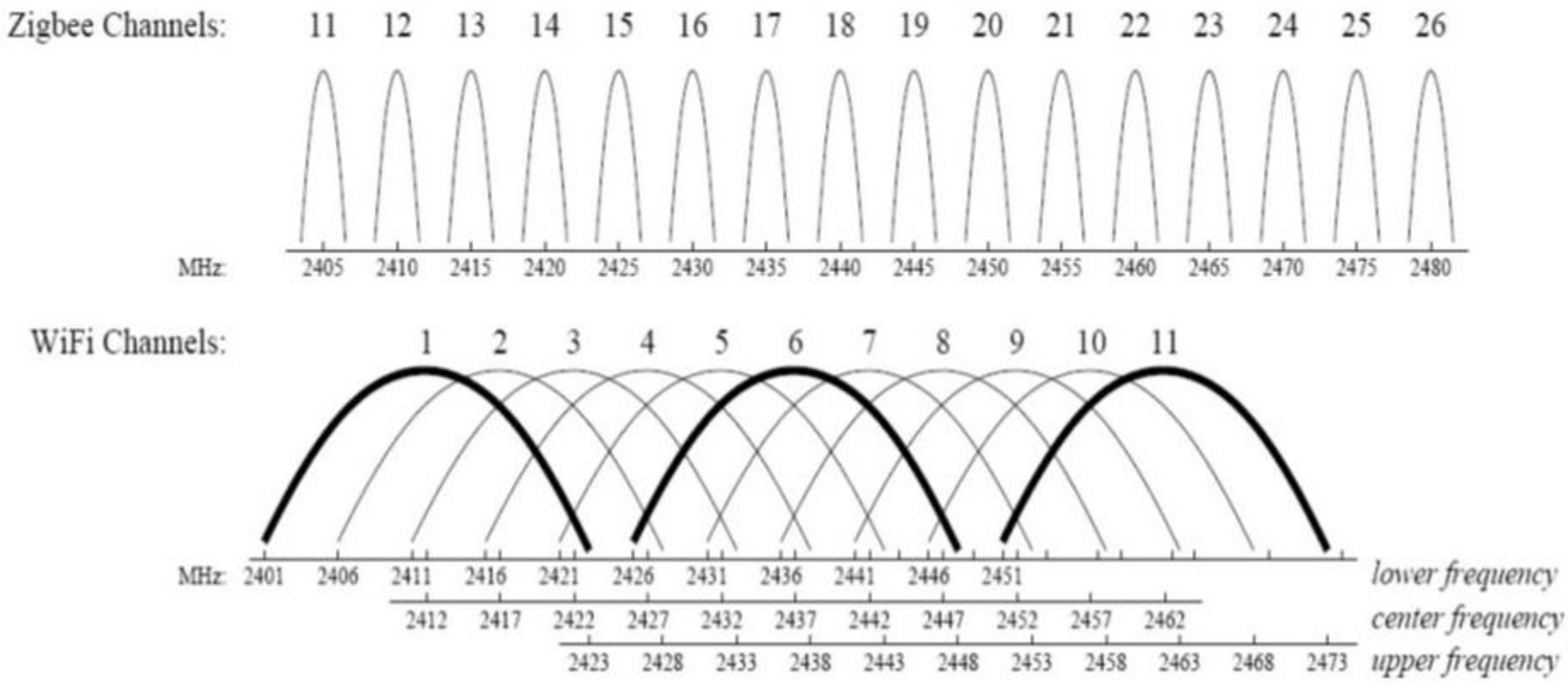
902-928 MHz band not available in Europe



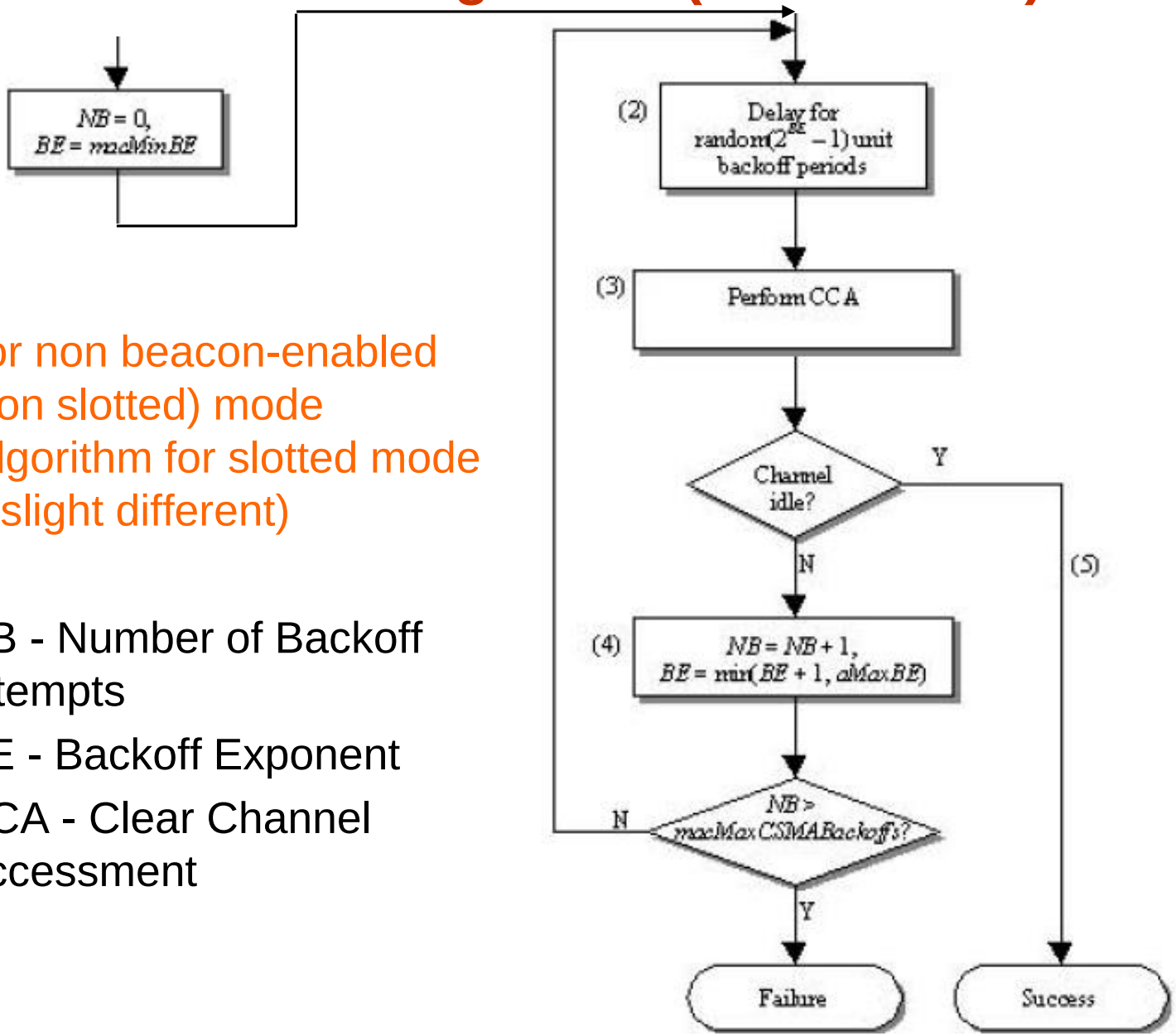


PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Coexistence with Wi-Fi networks



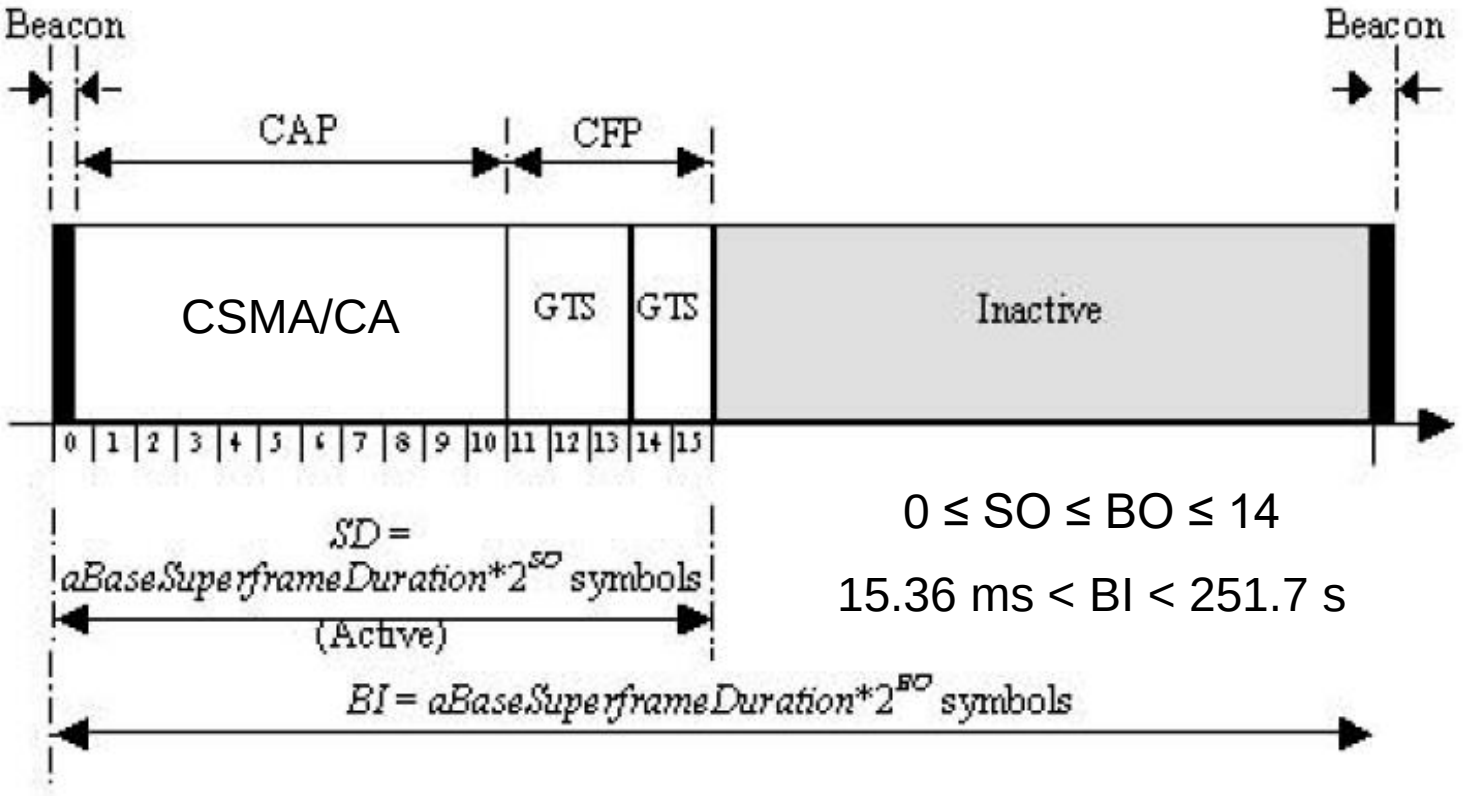
CSMA/CA Algorithm (Non Slotted)



- For non beacon-enabled (non slotted) mode (algorithm for slotted mode is slight different)

- NB - Number of Backoff attempts
- BE - Backoff Exponent
- CCA - Clear Channel Accessment

Superframe Structure (Beacon-enabled mode)



$0 \le SO \le BO \le 14$

15.36 ms < BI < 251.7 s

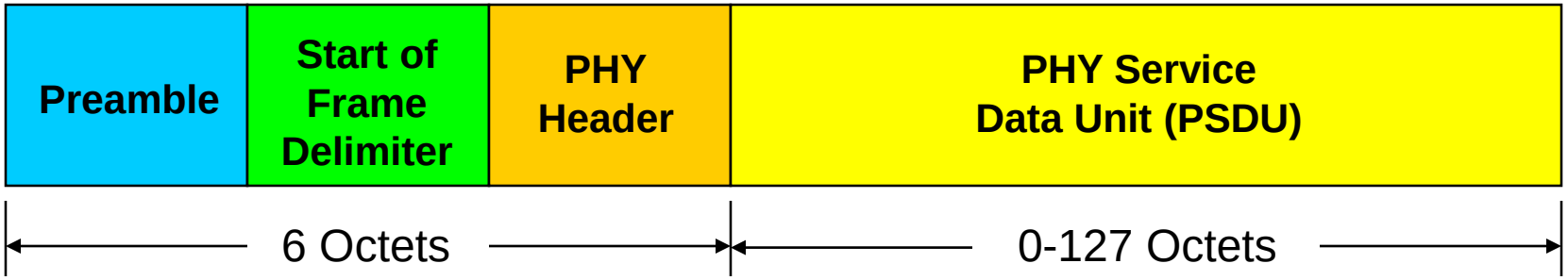
CAP - Contention Access Period
CFP - Contention Free Period
GTS - Guaranteed Time Slots

SD - Superframe Duration
SO - Superframe Order
BI - Beacon Interval
BO - Beacon Order

PHY Frame Format

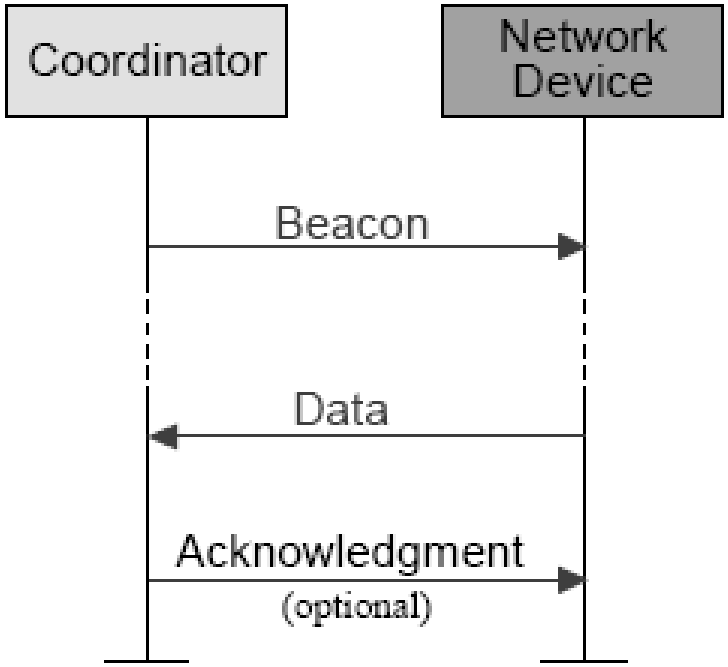
PHY Packet (PPDU) Fields

- Preamble (32 bits) – synchronization
- Start of Frame Delimiter (SFD) (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – payload

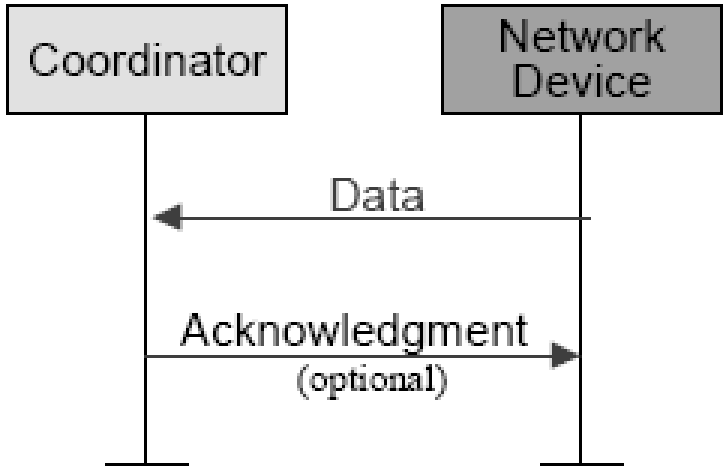


Data Transfer to a Coordinator

Beacon-enabled network

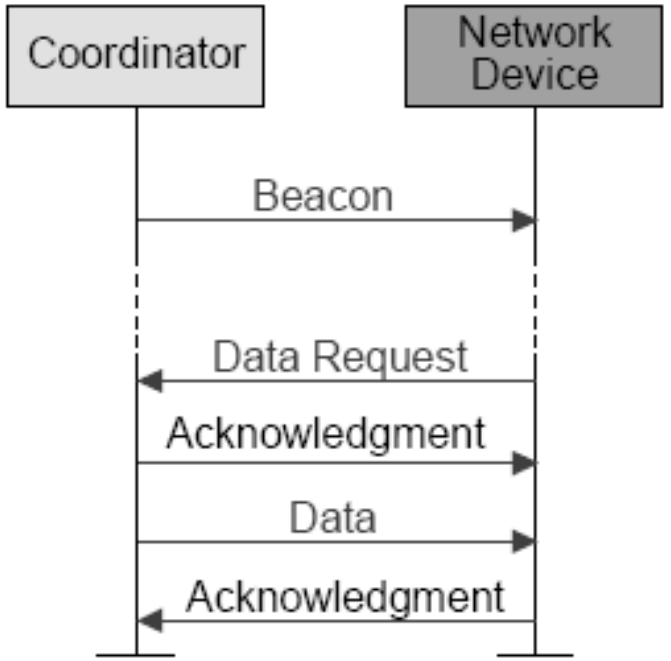


Non beacon-enabled network



Data Transfer from a Coordinator

- In a beacon-enabled network:
  - The coordinator indicates in the network beacon that the data message is pending
  - The device periodically wakes up and listens to the network beacon
  - If a message is pending, the device requests the data, using slotted CSMA-CA

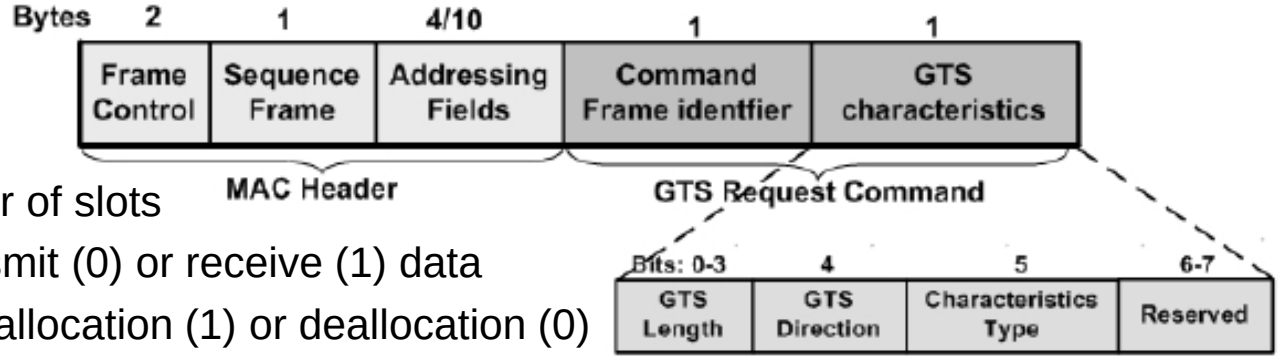


- In a non beacon-enabled network:
  - The coordinator stores the data and waits the appropriate device to make a Data Request.
  - If data are not pending, the coordinator transmits a data frame with zero-length payload.

Guaranteed Time Slot (GTS)

- Allows reservation of slots in a superframe to a given device
- Maximum of 7 GTSs at the same time.

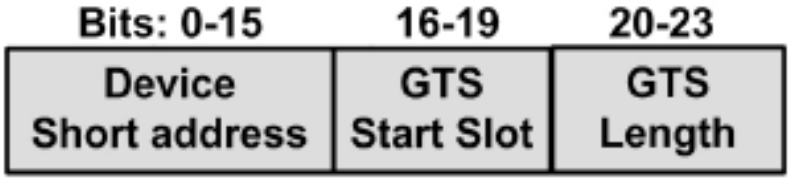
GTS Request



- GTS Length – number of slots
- GTS Direction – transmit (0) or receive (1) data
- Characteristic type – allocation (1) or deallocation (0)

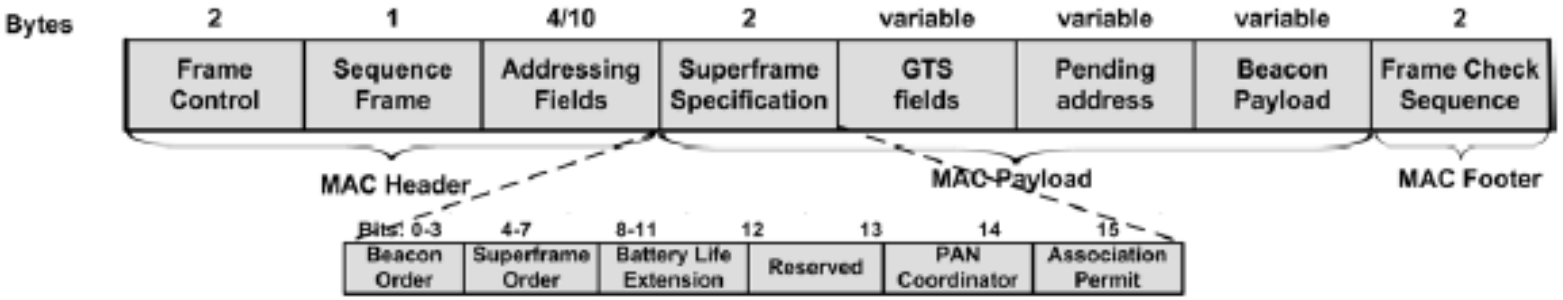
- The result of the GTS request is reported by the coordinator in the beacon frames using a GTS descriptor for each requesting device

GTS Descriptor

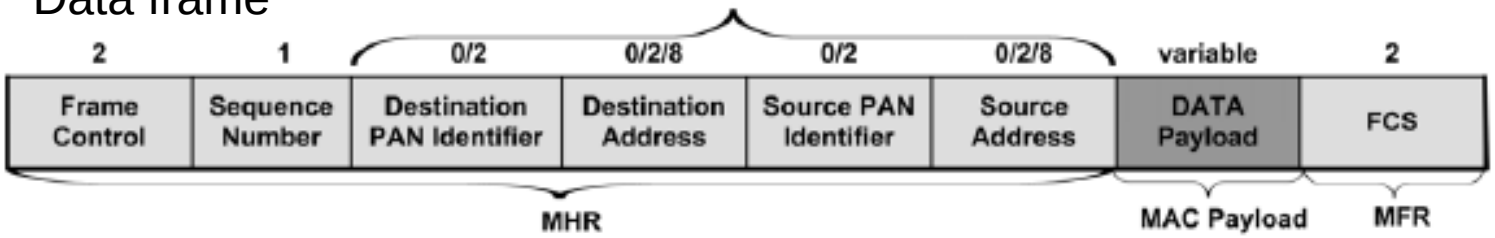


MAC Frame Formats

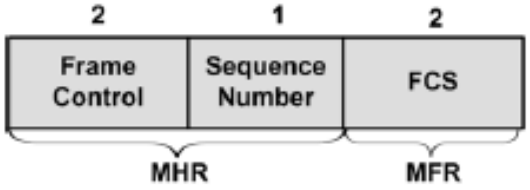
Beacon frame



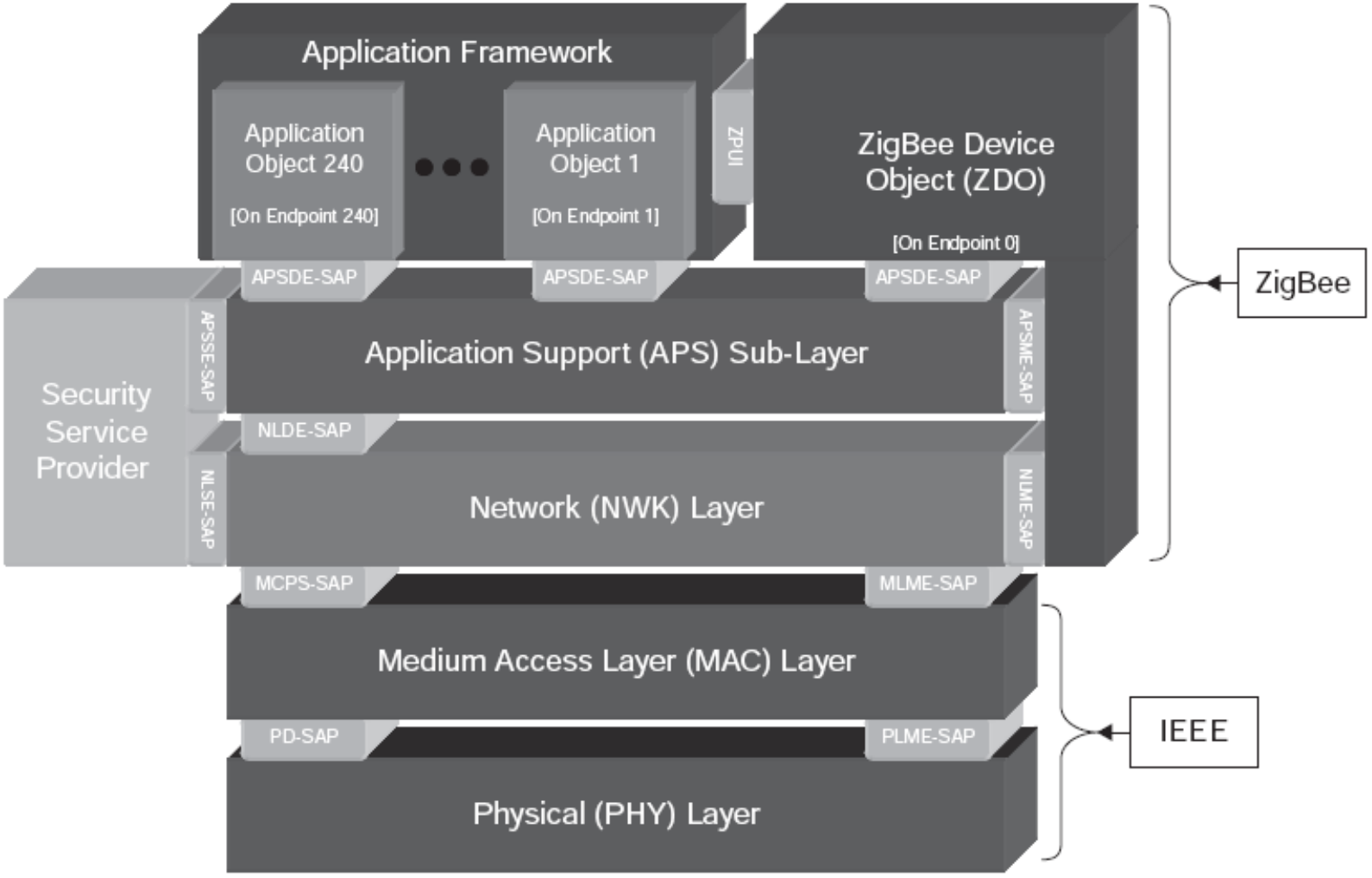
Data frame



ACK frame



ZigBee Stack



ZigBee Node Types

Coordinator (ZC)

- All ZigBee networks must have one (and only one) Coordinator.
  - In the Star topology, the Coordinator is the central node.
  - In the Tree and Mesh topologies, the Coordinator is the top (root) node in the network.

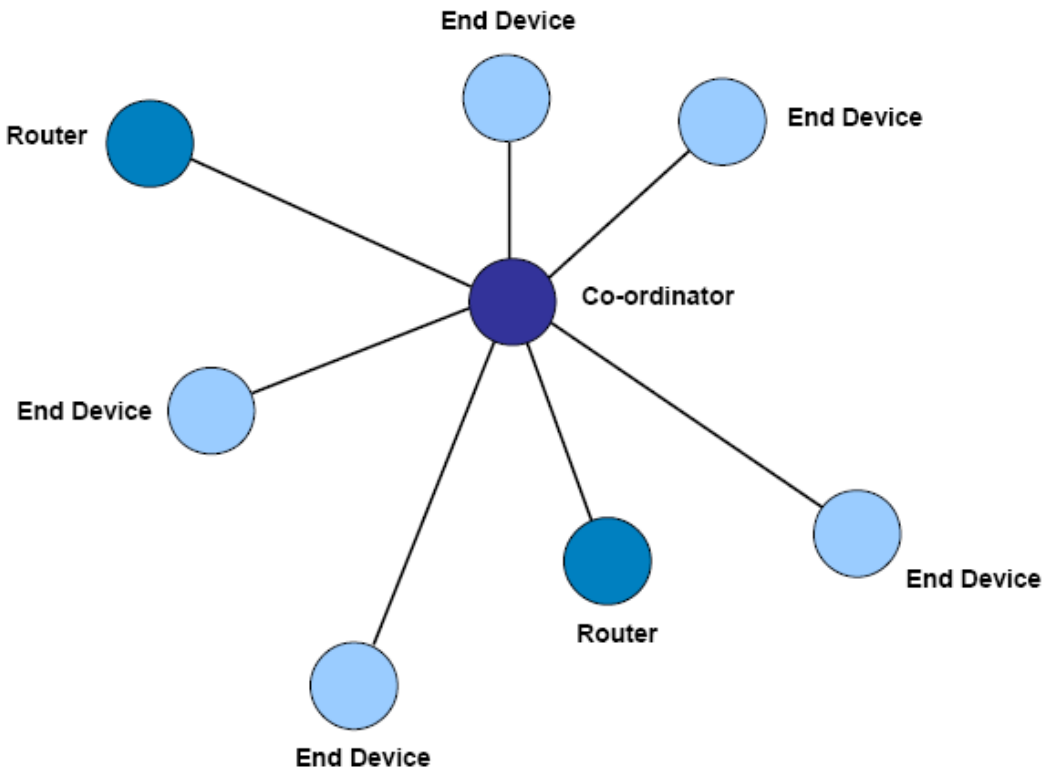
Router (ZR)

- Networks with Tree or Mesh topologies need at least one Router.
- The main tasks of a Router are:
  - Relays messages from one node to another.
  - Allow child nodes to connect to it.
- A Router cannot sleep.

End Device (ZED)

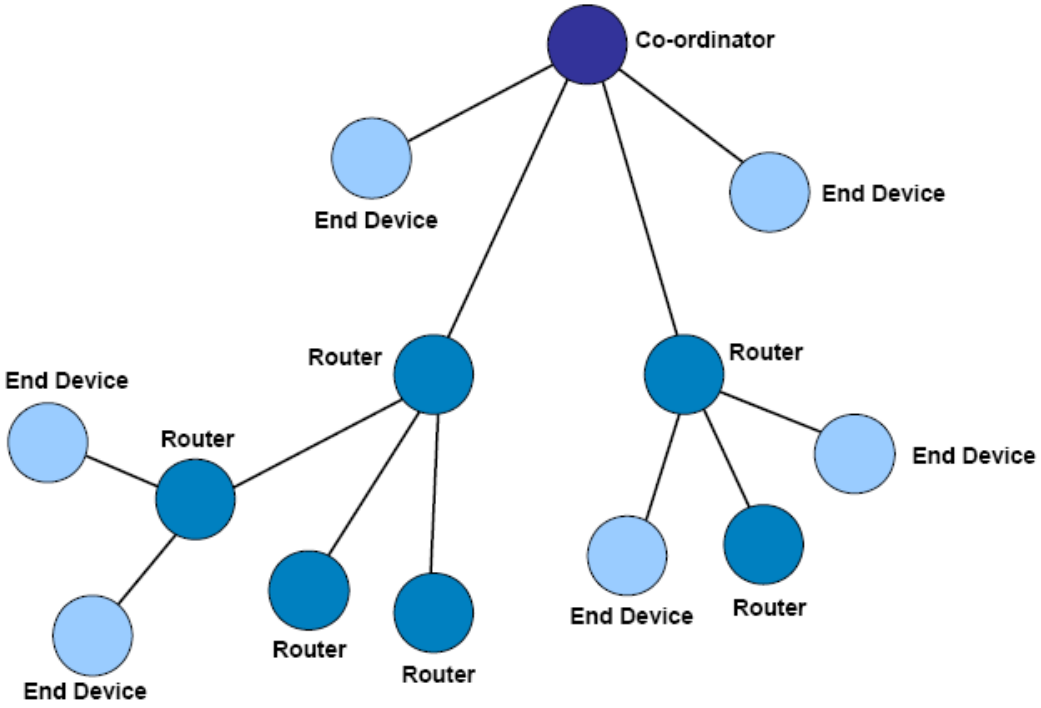
- End Devices are always located at the extremities of a network.
- An End Device can often be battery-powered and, when not transmitting or receiving, can sleep in order to conserve power.

Star Topology



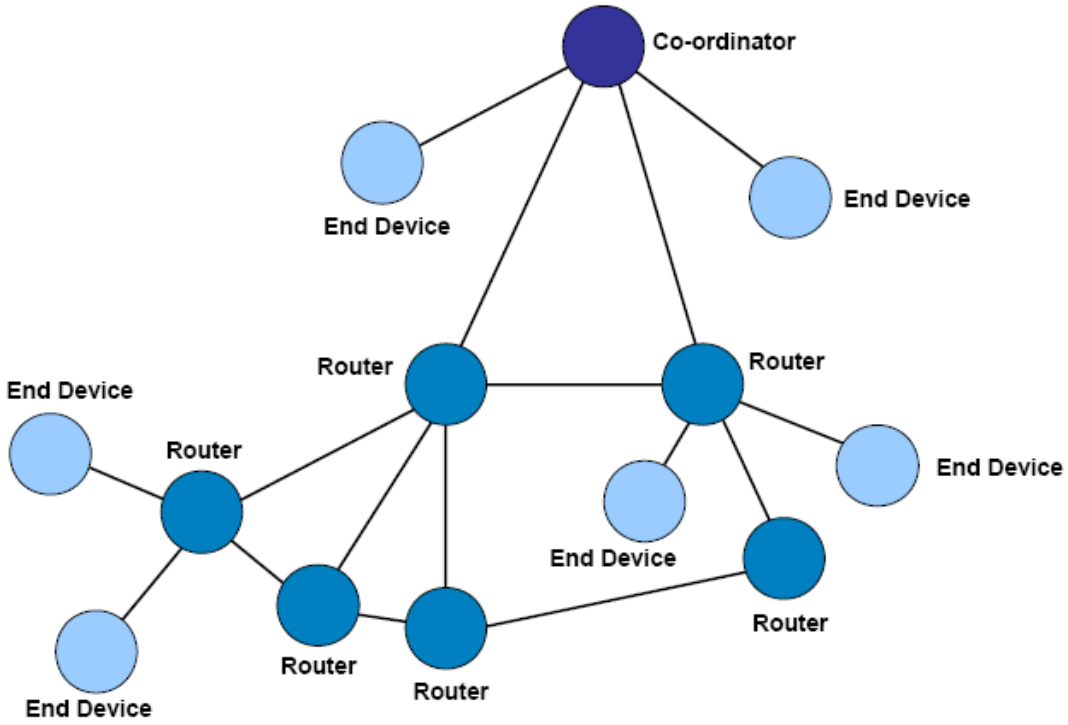
- The network has a central node (coordinator), which is linked to all other nodes in the network.
- All messages travel though the central node.

Tree Topology



- The network has a top node with a branch/leaf structure below.
- To reach its destination, a message travels up the tree (as far as necessary) and then down the tree.
- A disadvantage of this topology is that there is no alternative route if a necessary link fails.

Mesh Topology



- Router nodes within range of each other can communicate directly.
- Alternative routes can be found if a link fails or there is congestion.

ZigBee Coordinator Duties

- Starts the network formation.
- Selects the 802.15.4 channel on which the network will operate.
- Selects the extended and short PAN ID for the network.
- Decides on the stack profile to use (compile or run-time option).
- Acts as the Trust Center, storing security keys and using security services to authorize a device onto the network.
- Acts as a router for mesh routing.

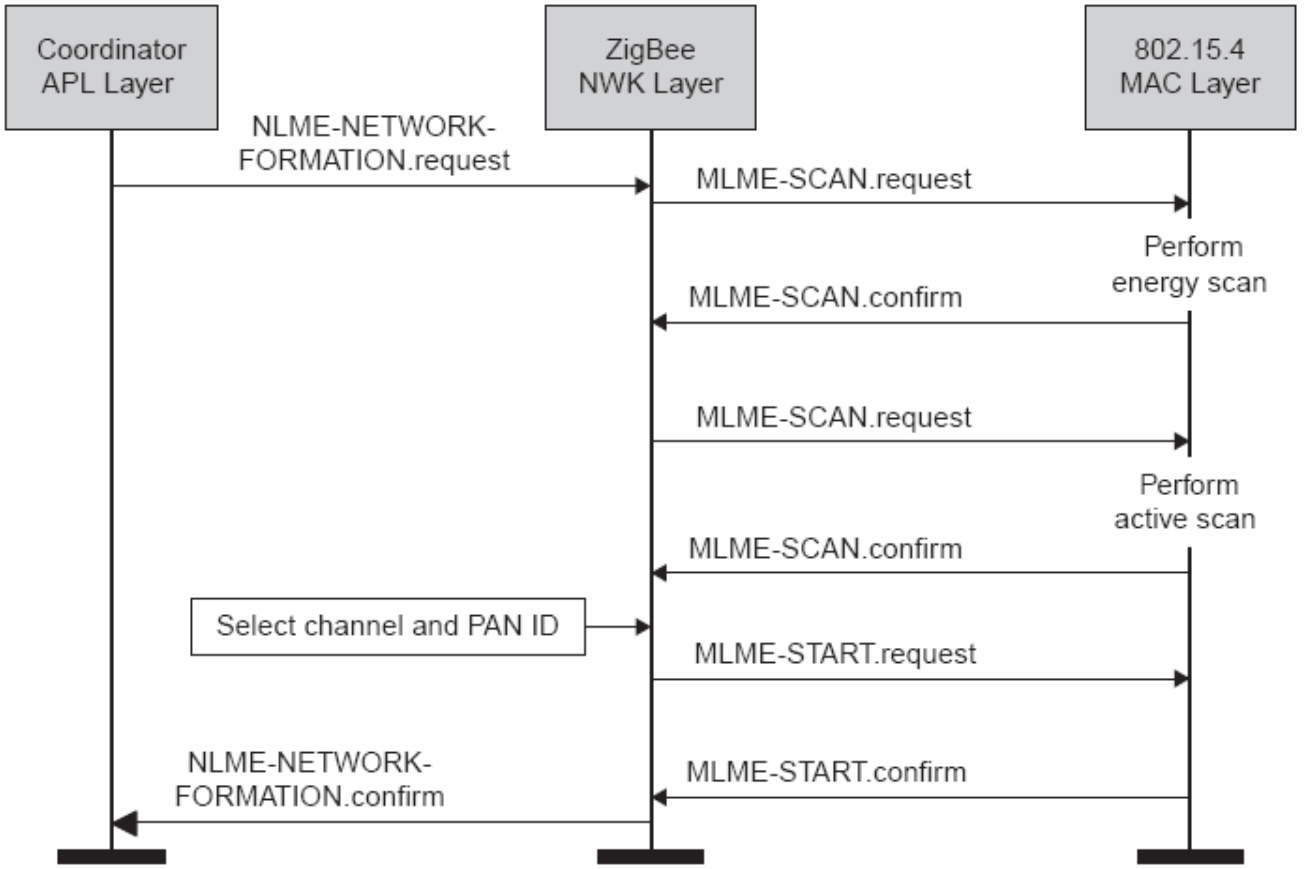
ZigBee Router Duties

- Finding and joining the “correct” network.
- Perpetuating broadcasts across the network.
- Participating in routing, including discovering and maintaining routes.
- Allowing other devices to join the network (if permit-join enabled).
- Storing packets addressed to sleeping children.

ZigBee End Device Duties

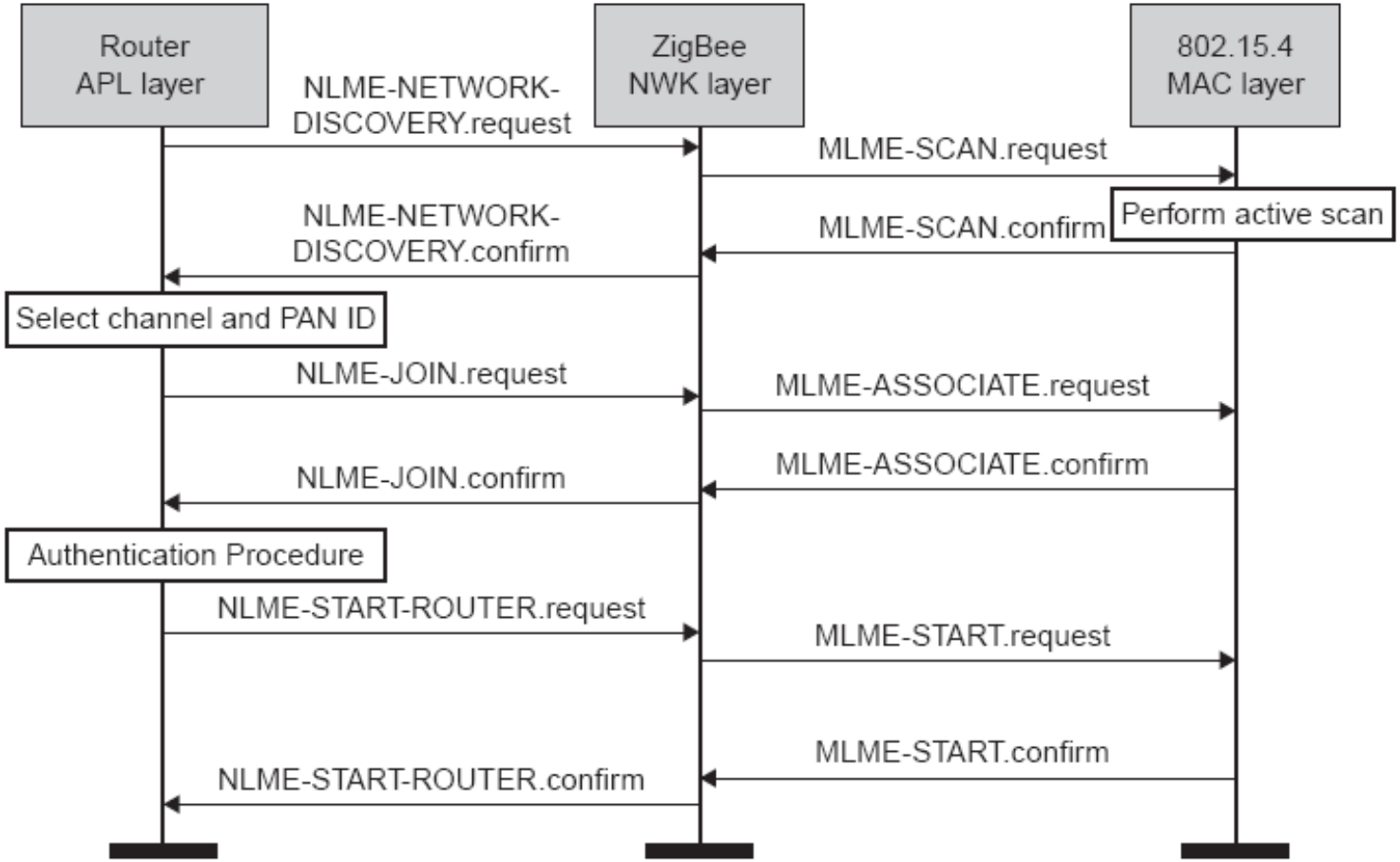
- Finding and joining the “correct” network.
- Polling their parents (data request) to see if any messages were sent to them while they were asleep.
- Finding a new parent if the link to the old parent is lost (NWK rejoin).
- Sleeping most of the time to conserve battery energy when not in use by the application.

ZC Network Formation



- Active scan - a MAC beacon request followed by zero or more beacon responses is used to discover what other networks are in the vicinity and ensure the coordinator does not form a network using an existing PAN ID.

ZR Network Joining Process



ZigBee Addressing

- ZigBee uses two addresses per node:
  - long address (64 bits) – unique in the world
  - short address (16 bits) – attributed at network joining
- Two source and two destination addressing fields:
  - MAC header – link nodes
  - NWK header – end nodes
- Short address assignment schemes:
  - Cskip - used by ZigBee (stack profile 0x01)
    - Deterministic assigned according to the node position in a symmetrical tree structure
    - Scalability of the network constrained to 10 hops
  - Stochastic - used by ZigBee Pro (stack profile 0x02)
    - Randomly assigned

ZigBee Routing

- Broadcasting
- Mesh routing
  - Based on AODV (Ad hoc On-Demand Distance Vector) routing protocol
  - Requires a routing table on each router
  - The route discovering process is performed on demand
  - A route is kept until it fails or it is removed from the routing table
  - When an existing route fails, the originating node is informed and starts a new route discovery (self-healing)
- Tree routing (only in stack profile 0x01)
  - Based on the Cskip addressing
- Source routing (only in stack profile 0x02)
  - Routes are stored in a single node and sent within the packets
  - Limited to a maximum of 5 hops

Application Profiles

- Collections of common definitions and protocols that allow various devices to work together in a particular domain
- Allow device interoperability across different manufacturers
- Each profile defines device types and required functionality
- Profiles can be Public (developed and maintained by the ZigBee Alliance) or Private (manufacturer specific)
- Each public or private profile has a name and a 16-bit numeric identifier to tag its messages.
  - For example, the Smart Energy profile uses 0x0109.
  - Any device that wants to support the Smart Energy profile is required to provide certain standard functions and to identify its messages with 0x0109 to all other devices.

Application Profiles

- Some public profiles
  - Health Care
  - Home Automation
  - Building Automation
  - Smart Energy
- Examples of use
  - The Smart Energy profile allows different brands of electric meters, thermostats, appliances, and in-home display units to share a common language.
  - Any ZigBee Health Care-certified patient sensor can communicate medical data to any other brand of Heath Care-certified patient monitor

Example: Devices of Home Automation Profile