MOBILE & CYBER-PHYSICAL SYSTEMS

THE IEEE 802.15.4 STANDARD

STEFANO CHESSA

1

(1) EXPLICIT SYNCRONIZATION

LEARNING OBJECTIVES

Physical layer of the IEEE 802.15.4 standard	MAC layer of the IEEE 802.15.4 standard	Support for dynamic network formation

2

THE IEEE 802.15.4 STANDARD

Specification of the physical and MAC layers for low-rate Wireless Personal Area Networks (PAN).

Infrastructure-less

Short range

The Physical layer can coexist with IEEE 802.11 and IEEE 802.15.1 (Bluetooth),…

Licence-free frequency bands:

- 868–868.6 MHz (e.g., Europe) with a data rate of 20 kbps;
- 902–928 MHz (e.g., North America) with a data rate of 40 kbps; or
- 2400–2483.5 MHz (worldwide) with a data rate of 250 kbps.

3

PHYSICAL LAYER

4

PHISICAL LAYER (L1)[bits] : - Data service : T/R of PPDU thru physical medium
- Management service : RADIO T/R & energy efficience implementation
  - Energy Detection
  - Link quality indicator
  - Channel selection

PHYSICAL LAYER

1) **Data Service**

- Transmission/Reception of *PHY Protocol Data Unit* (PPDU) through the physical medium.

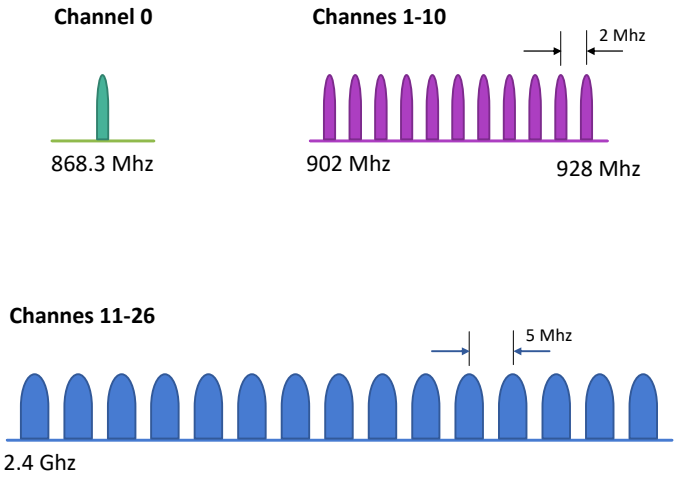
2) **Management Service**

- Radio transceiver activation/deactivation (to implement policies of energy efficiency)
- Energy Detection - ED
- Link Quality Indicator – LQI
- Channel Selection
- Clear Channel Assessment – CCA
- PHY-PIB (PHY PAN Information Base) Configuration

3) Used in 2.4 Ghz, 16 Frequency band
=> ≤16 ZigBee Networks

5

PHYSICAL LAYER



6

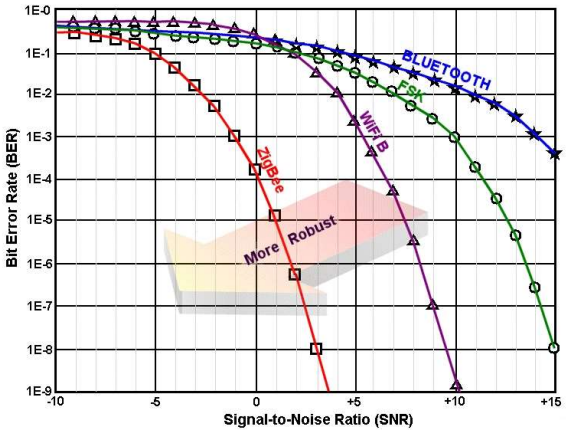
PHYSICAL LAYER: EXAMPLE

Frequency band: 868 MHz
bit rate: 20 kbps
Symbols: binary
1 channel centered on 868.3 MHz
Maximum packet size (bytes): 127

7

$SNR = \frac{Power}{noise} \Rightarrow 20 \cdot \log(SNR) = 20 \cdot \log\left(\frac{signal}{noise}\right)$

PHYSICAL LAYER: PERFORMANCE



BER: P that a bit is received in error at the receiver

excellent performance in low SNR environments

8

- **SNR** vs **BER** tradeoff: how implicit is information in electro waves
  - given a phisical layer: increase power → increase SNR(quality of the signal) → decrease BER (send bits → electro waves to the medium)
- **given SNR**: choose a physucal layer that meets BER requirement, **giving highest throughput**

- Electrical signal = PORTANTE
- ONDA PORTANTE = tecnique used in telecommunication for modulation of the signal

ED: ENERGY DETECTION

PHYSICAL LAYER: ENERGY DETECTION

Used to find a free channel and for carrier sense

Estimation time for ED = average over 8 symbols interval

Detection threshold at 10dB above the sensitivity level

ED result given in a byte

10

PHYSICAL LAYER: LINK QUALITY INDICATOR

Used in multi-hop routing

Link Quality Indicator (LQI) indicates the quality of data packets that are received by a node.

It is based on ED, or on the signal/noise ratio, or both.

It is assessed each time a packet is received. (CALCULATED)

It must have at least 8 different levels.

The estimated value for LQI is forwarded to the network and application layers.

11

PHYSICAL LAYER: CHANNEL ASSESSMENT

CHANNEL ASSESMENT:
- to find if channel is busy

Objective: to detect if the channel is busy.

3 modes:

- Mode 1: use ED; if the energy level exceeds the detection threshold, then channel busy.
- Mode 2: Carrier Sense, the channel is busy if the detected signal has the same characteristics as the sender.
- Mode 3: Combination of modes 1 et 2 (AND/OR).

12

DATASERVICE & PHYSICAL LAYER

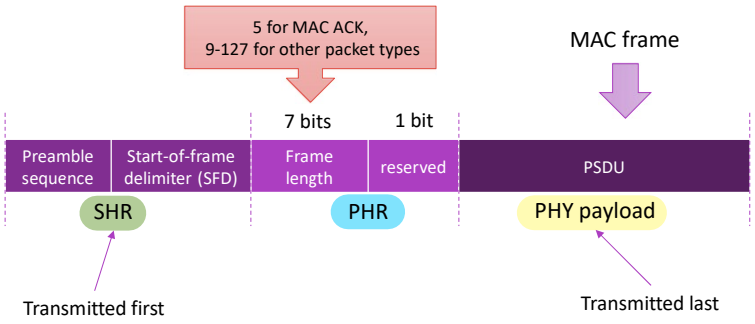
PHYSICAL LAYER: DATA SERVICES

- In the PHY layer: PPDU (PHY Protocol Data Unit)
- PPDU (PHY PDU) reports the result of the transmission to the upper layer (success or fail)
- Reasons for transmission failure:
  - radio transceiver out of order
  - radio transceiver is in the reception mode
  - radio transceiver busy

13

PHYSICAL LAYER: THE FRAME

FRAME



1) • SHR (Synchronization Header): synchronisation with the receiver
2) • PHR (PHY Header): information about the frame length
3) • PHY Payload: the MAC frame

14

END OF PHYSICAL LAYER L1

MAC LAYER

"Data Link" -> L2 -> Frame

15

MAC LAYER SERVICES: this standr supports ≠ topology and organization ways of the network
=> ≠ services

MAC LAYER SERVICES

1) **Data services**
- transmission and reception of MAC frames (MPDU) across the physical layer.

2) **Management services**
1) • synchronization of the communications;
2) • channel access;
3) • management of guaranteed time slots;
4) • association and disassociation of devices.

3) **Security services**
- Data encryption
- Access control
- Frame integrity
- Sequential freshness

16

2 TYPES OF DEVICES

MAC LAYER: DEVICES

- low powered devices

1) **Reduced Function Devices (RFDs)** → operate at the boundary of the network
- End-devices with reduced processing, memory, and communication capabilities
  - simple sensors or actuators like light switches, lamps and similar devices
- Implement a reduced set of functions of the MAC layer:
  - associate to an existing network
  - RFD depend on FFDs for communication.
  - one RFD can be associated to only one FFD at a time.

• they rely on FFD to be connected to the rest of the network
• Implement only MANDATORY part of the standard (no optionally part)

2) **Full Function Devices (FFDs)**
- Implement the full MAC layer
- Act as the Personal Area Network (PAN) coordinator or as a generic coordinator of a set of RFDs
- The PAN coordinator sets up and manages the network:
  - selects the PAN identifier
  - manages associations or disassociation of devices.

may operate as coordinator or rather
=> may implement optional functionalities

17

- Basically 2 topologies at the MAC LAYER => (Zigbee uses those 2 to implement its 3 topology: star, tree, P2P)

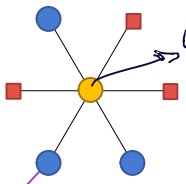
MAC LAYER TOPOLOGIES: STAR

One FFD is the PAN coordinator; the other nodes behave as RFDs

The PAN coordinator synchronizes all the communications in the network.

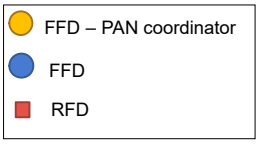
Different PANs have different identifiers and are independent

(1) STAR



- at the boundary even if devices are FFD, operates as RFD

Routers act as RFD!



18

(2)
- P2P topology to construct arbitrary-sized topology (multi-hop), over this topology can build a tree in ZigBee // generic mesh net of ZigBee

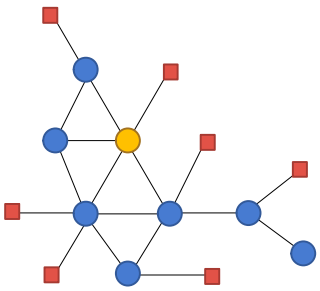
MAC LAYER TOPOLOGIES: PEER TO PEER

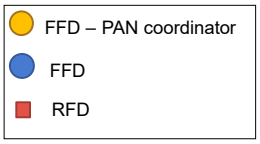
(2) P2P

Each FFD communicates with any other device within its radio range

One FFD is the PAN coordinator; the other FFD are routers

Each RFD acts as end-device and it is connected to one FFD





- RFD always at boundary, always depend on router // coordinator to connect

19

CHANNEL ACCESS

• KEY ELEMENT: possibility to configure the network with/without SUPERFRAME

• energy efficiency is implicit cuz is enforced the sync by MAC LAYER
→ and this enforce also the idle/activity periods of NET INTERFACE

• coordinator forces syncronization of all the nodes

MAC LAYER: CHANNEL ACCESS

with a superframe structure

- used in star topologies
  - it can also be used in peer to peer topologies organized in trees
- enforces synchronization of devices
  - enables power savings of the devices.

without a superframe structure.

- is more general
- used to support communications in arbitrary peer to peer topologies

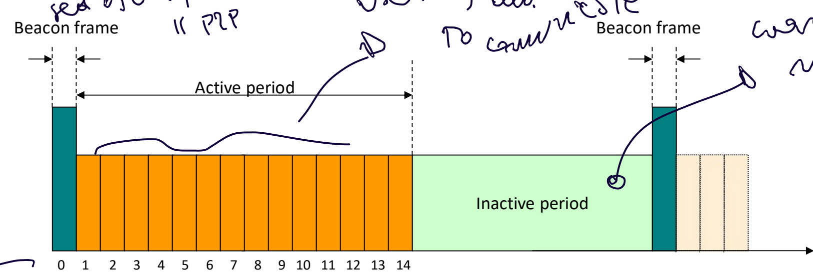
• no syncronization enforced by mac layer
=> MAC LAYER doesn't support you with energy efficience operations
=> up to you

20

CHANNEL ACCESS WITH SUPERFRAME

- The time slots are equally sized
- The first time slots is the beacon frame
  - It is sent by the PAN coordinator to begin the superframe.
- The beacons are used to:
  - Identify the PAN.
  - Synchronize the devices in the PAN,
  - Communicate the structure of the superframe. → ACTIVE + INACTIVE period
- The end devices can communicate with the coordinator in the remaining time slots.

end dev. communicate in active slots periods



sed by coord is sent || P2P
used by dev. to communicate
coord & dev may turn off the radio

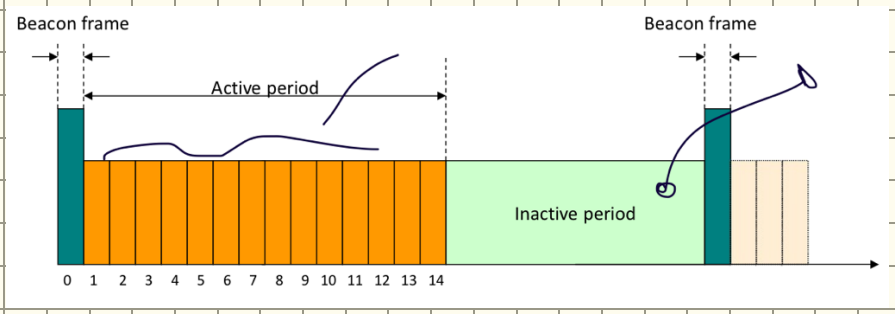
21

Time of the radio's acc

• SLOTS: same size; define PAN
up to 16 SLOTS
ACTIVE + INACTIVE: set by coord via BEACON: if ... is a ...
- Coord SAN ... via Beacon: frame describe ...

CHANNEL ACCES VIA SUPERFRAME

- time of the nodes organized according to the diagram
- At a given time, COORDINATOR initiates ACTIVITY PERIOD of the network by sending a BEACON
- BEACON: just a frame (mac layer frame) containing informations describing the network: period of activity of the network, duration of inactive/active period, network address, other infos relevant.
- after the beacon follows: ACTIVE PERIOD:
  - divided in slots (up to 16): 1 slot reserved for the beacon, the others may be used by other devices to communicate:
    1) Communicate to the coordinator
    2) by the coordinator to send the frame to the associated devices
- after active period follows: INACTIVE PERIOD:
  - in which coord and other devices may TURN-OFF the radio



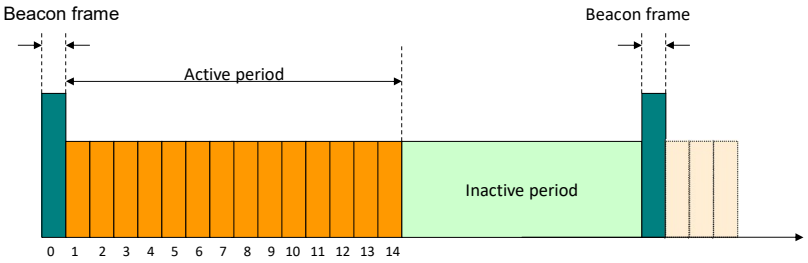
- Duration of active and inactive periods is fixed for all:
  - coord. decides them and advertize them in the beacon
- Other nodes ∈ Network should obey

- if network = star topology => synchronization is simple:
  1) Coordinator emits the beacon
  2) all the nodes in the star receive the beacon
  3) after the beacon they know they may communicate in one of these slots
  4) And they can turn-off the radio in the inactive period
- if network = P2P (possibly multi-hop network) =>
  1) Coordinator (still) send the beacon (and decides active/inactive period duration)
  2) All the routers associated to the network, take the same parameter
  3) And each router emits a copy of the beacon: to sync its neighbor

REMIND: - slots same size, beacon frame in the 1st one
- beacon identifies the PAN, sync the devices, gives info of the SUPERFRAME structure

CHANNEL ACCESS WITH SUPERFRAME

- The superframe comprises an active and an inactive portion.
- All the communications happen during the active portion
  - the PAN coordinator (and the connected devices) may enter a low power (sleep) mode during the inactive portion.
- The active portion comprises up to 16 time slots.



22

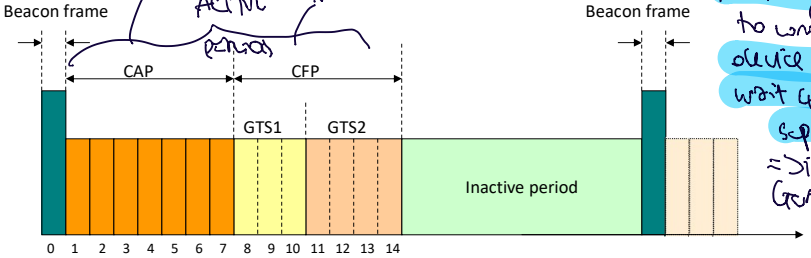
- ACTIVE PERIOD can be further DIVIDED in: (1) (2)
  - this protocol allows to end devices to request to coord for guaranteed time slots
    => slots reserved 4 one device, so at each superframe those slots are always for that device (others cannot communicate in those time slots that are guaranteed

CHANNEL ACCESS WITH SUPERFRAME

=> 4th comes contention slots => CSMA/CA
=> other contention free periods, can be divided in GROUP of guarantee time slots:
- every group is assigned to a different device: ex: if a device is an app that requires to communicate at constant rate, to enforce reliability of this app, make sure that every superframe the app have the possibility to communicate.

- The time slots in the active portion are divided into:
  1) • Contention Access Period (CAP) and
  2) • A (optional) Contention Free Period (CFP).

contention slots: CSMA
divided in 2 slots



- this can be guaranteed with contention or if with contention there are too many devices wants to communicate, some device will have to wait 4 the next superframe => just stuck with GUARANTEES =>

23

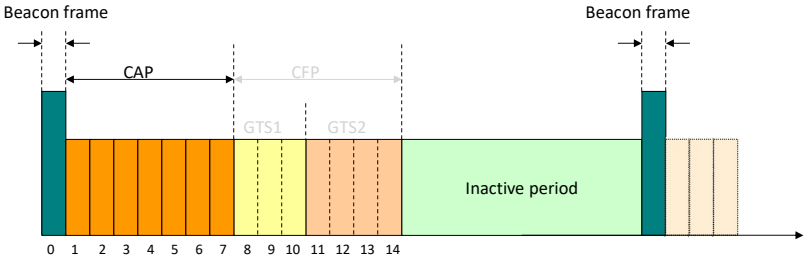
- the application may reserve part of the slots before ends by requesting these slots to the coord, the coord informs in the beacon frame that there are GTS, so all devices are informed of GTS presence => not interference where GTS comes and that app will communicate in these slots => no need CSMA/CA, just transmit

- CONTENTION ACCESS PERIOD (CAP): - should always include at least 1 slot:
  - so device may req. to coord GTS but they cannot occupy all the slots => AT LEAST 1 CONTENTION SLOT SHOULD REMAIN
  => because contention slots are used also for MANTAINANCE OF THE NETWORK
  (es. device wants to join, make the request to coord using the contention slot)

CHANNEL ACCESS WITH SUPERFRAME

The Contention Access Period (CAP) period:

- comprises up to 15 time slots
- the devices compete for channel access using a standard slotted CSMA-CA protocol
  - a device shall wait for a random number of slots first.
  - if the slot is busy the device shall wait for another random number of slots before trying again.
  - If the channel is idle, the device can transmit.
- Objective: gain access to the medium (CSMA-CA); once the transmission starts, the node keeps the medium until the end of the frame



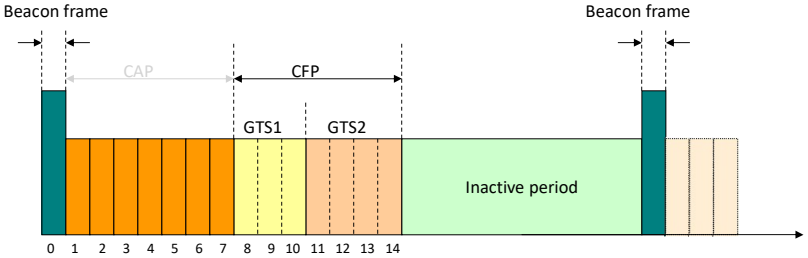
24

- NB: IT'S ALWAYS THE COORDINATOR THAT DECIDES THE ALLOCATION FOR CONTENTION FREE SLOTS

CHANNEL ACCESS WITH SUPERFRAME

The CFP period is optional: → used for app requiring low latency

- for low-latency applications or applications with specific data bandwidth.
- occupies the last time slots of the active period
- divided into Guaranteed Time Slots or GTS
  - Each GTS assigned by the PAN coordinator to a specific application
  - The application accesses the GTS without contention
  - The GTS may comprise more than one time slots.
- medium access without CSMA-CA
- max. 7 GTS within a CFP (each GTS may have one or more time slot)



25

- if you're using GTS => you're to close your communication in the slot assigned to you (no when you want)

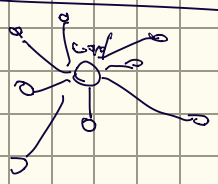
How does it work the access in contention access period (CAP)?

=> its CSMA/CA: a device picks up at random 1 contention slot, when that slot arrives implements carrier sense, then implements collision avoidance with RTS/CTS and if it is free to transmits GO

=> In the slot there's also the time to receive the ack, within the same slot

if channel is busy => then the device waits for another slot and if contention slots are over => then will have to wait to the next superframe

- Superframe works good in a star ntwrk topology



=> in this way coord. enforce energy efficiency

- Superframe defines DC of coordinator's radio
- End devices' DC may be lower, cuz are not oblished to wake up during the activity period
  => can keep off radio for long period, then wake up again, wait for the beacon, communicates during the contention slot, turn off the radio
- => this primarily defines coordinator's DC: coord have to turn on the radio on at the beginning of each superframe

- is possible to use superframe structure even in multi-hop network (PAN)
  => every router initiate the superframe emitting the copy of the beacon

  => if two routers are adjacent, they cannot initiate emitting the beacon at the same time, cuz they will collide
  => 2 routers should find a time to send their beacon
  -> "activity period of 2 routers should happen in the inactivity period of the other"

⇓

- to guarantee this, routers and coordinator should implement a protocol to decide when initiate their activity period => both protocol ≠ ZigBee spec => up to you (in P2P NET)

CHANNEL ACCESS WITH SUPERFRAME

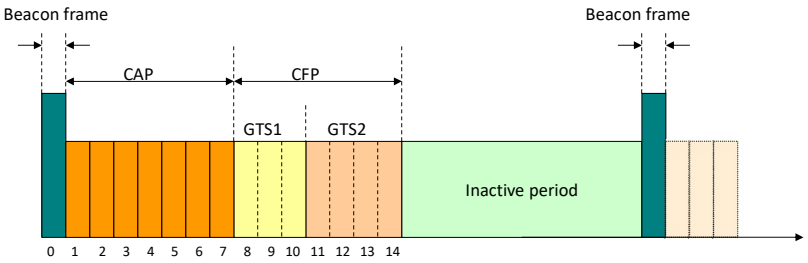
The CFP does not occupy all the time slots

the CAP period is necessary for the network maintenance

- to manage the association/disassociation protocols,
- allocation of GTS, …

All contention-based transactions shall be completed before the CFP.

A device transmitting in a GTS shall complete its transmission within its GTS.



26

FRAME TYPE

4 frame types:

1) Beacon frame
2) Data frame
3) Acknowledgement frame
4) Command frame (MAC)

27

CHANNEL ACCESS WITH SUPERFRAME

Each PAN coordinator creates its own superframes:

- Active periods of the superframes have always the same length
- The coordinator initiates the superframe by sending a beacon

instructing the nodes eager to emit beacon frame periodically with the info

Peer to peer topologies:

- All routers in a PAN use the same parameters of the superframe (chosen by the coordinator)

copy beacon

28

- NETWORK CAN OPERATE WITHOUT SUPERFRAME: in this case to support a MAC with lowest efficiency.
- In principle devices should keep radio on all the time, it's up to you implement energy efficiency strategy

CHANNEL ACCESS WITHOUT SUPERFRAME

The PAN coordinator may avoid the use of the superframe structure

- The PAN is called *non beacon-enabled*

No beacons or slots: communication based on unslotted CSMA-CA protocol.

The coordinators (PAN coordinator and routers) are always on and ready to receive data from the end-devices

Data transfer from coordinators to end-devices is poll-based

- The end device periodically wakes up and polls the coordinator for pending messages.
- The coordinator then either sends back the pending messages or signals that no message is pending.

→ interrogo, chiedo

31

- CUT WITHOUT superframe there are no beacons => there are not SLOTS => CSMA/CA:

CSMA/CA: - when you want to transmit, listen to the channel, if is free, you sent RTS, if you receive CTS => TRANSMIT

=> Conseguence: Coord and router should keep radio on unless you find a way to let them turn off radio

- End devices (RFDs), they may have low DC, cuz don't have to keep radio always on, => have ARBITRARY DC: when they turn on their radio, contact the router and then operate

- PROBLEM if coord/rout wants send frame to a turned off radio device => need something PROTOCOL

DATA TRANSFER MODES

Three types of data transfer:

1. End-device to coordinator (or router)
2. Coordinator (or router) to end-device
3. Peer to peer.

The star topology uses only types 1. and 2.

- the data transfers can happen only between the PAN coordinator and the other devices.

The peer to peer topology all the three types of data transfer are possible

- data can be exchanged between any pair of devices.

Different implementations for the beacon-enabled and non-beacon enabled cases

32

1ST CASE: => data transfer with the beacon-enabled network (superframe): END-DEVICE → COORD, or (ROUTER)
- star topology
- initiated by coord (router)

DATA TRANSFER IN BEACON ENABLED NETWORKS

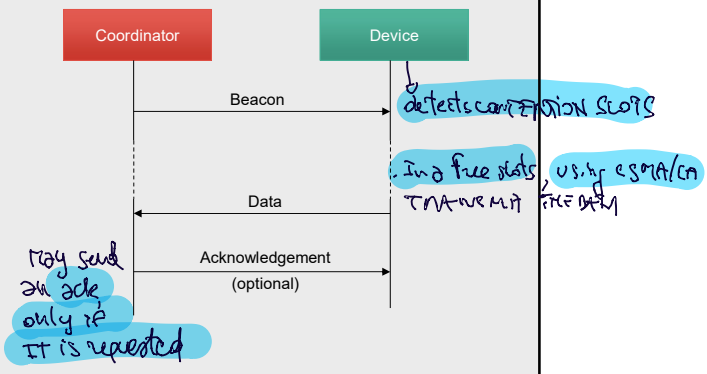
Data transfer from an end device to a coordinator :

The end device first waits for the network beacon to synchronize with the superframe.

If it owns a GTS it uses it without contention
↳ Guaranteed time slot

Else it transmits the data frame to the coordinator using the slotted CSMA-CA protocol in one of the frames in the CAP period.

The coordinator may optionally send an acknowledgement



33

CASE: beacon-enabled network with superframe: coord → END DEVICE

- more complex: cet during the activity period, the end device may be off (turns on the radio at any time)

(AF): the beacon, beyond containing params of the network, contains the LIST of pending msgs u end devices. (with the flag in this list transmitted in the beacon)

DATA TRANSFER IN BEACON ENABLED NETWORKS

Data transfer from a coordinator to an end device:

The coordinator stores the message and signals that the message is pending in the beacon;

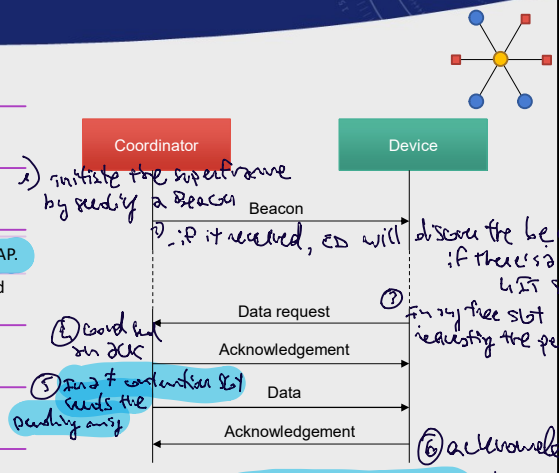
The end-device sleeps most of the time and it occasionally listens to the beacon to check for pending messages.

When it notices that a message is pending, it requests the message to the coordinator — Data request message in the CAP. It is immediately acknowledged by the coordinator

The coordinator sends the pending message in a successive slot of the CAP.

The device sends an acknowledgment frame in a successive time slot (mandatory)

The coordinator removes the pending message from its list.



- NB: In this communication, ACKs are MANDATORY

34

- NB: if END DEV is off when coord snd beacon → notify happens, data remains pendy (will resend it next its activity period) (bc coord wants to be sure that pendy msg is received, so it can throw it away)
- IF PROTOCOL FAILS, DATA REMAINS PENDING

DATA TRANSFER IN BEACON ENABLED NETWORKS

(3rd) BEACON-ENABLED NTWRK (using Superframe in P2P)

Peer-to-peer data transfers:

Between the coordinator (or a router) and an end-device one of the previous schemes is used.

Between two end-devices: not possible!

- Two end-devices cannot communicate directly

Between the coordinator and a router (or between two routers):

- The sender must first synchronize with the destination beacon and act as an end device.
- The measures to be taken in order to synchronize coordinators are beyond the scope of the IEEE 802.15.4 standard.

35

BEACON-ENABLED NTWRK - USING SUPERFRAME IN P2P NETWORK

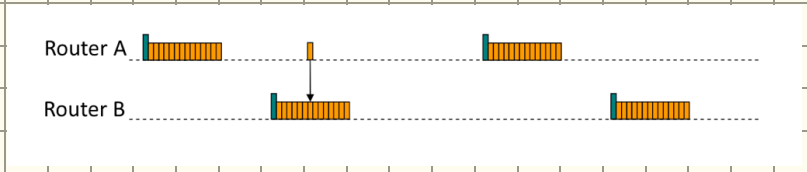
- Net with arbitrary topology (P2P)

- Need to support communication among routers, routers/coordinator: NOT possible end device -> end device

  - PROBLEMATIC : cuz the transmitter is a router (having its own activity period)
    - reciev is another router (≠ active period)
    - => received maybe not be ON during active period of the transmitter (and vicevesa)

- SITUATION:
  - 2 routers are adjacent, in range of each other
  - both routers emit their own beacon
  - " " have their active period
  - they must NOT be sync, otherwise they will collide

    => similar to S-MAC



- When router (A) want to transmit to (B):
  - turns the radio on during the active period of (B)
  - waits for the beacon of (B)
  - finds a free contention slot during active period of (B)
  - then transmits, using CSMA/CA

- (A) and (B) need to implement a protocol to agree when to transmit their own beacon (to avoid collisions) => this protocol is not part of the standard

- FROM ED → COORD in network WITHOUT SUPERFRAME (aka non-beacon-enabled records)
  - assumption: routers or coordinators ALWAYS ON
    - end devices turn on when they want
  - TRASMISSION: routers/coord always on => end devices just send data using CSMA/CA - ack optional

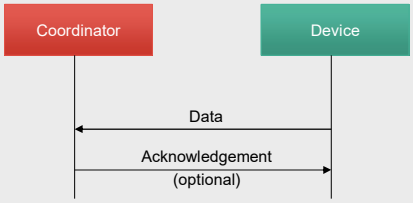
DATA TRANSFER IN NON BEACON-ENABLED NETWORKS

Data transfer from an end device to a coordinator: /router

the end device simply transmits its data frame to the coordinator using unslotted CSMA-CA.

The coordinator must be always active...

The coordinator acknowledges the successful reception of the data by transmitting an optional acknowledgment frame.



36

- also here ASSUMPTION: routers/coord (FFD) always ON

- From router/coord → end devices
- end-device may be RFD
- there's no beacon => no way for the transmitter to advertise presence of pending message
1. IT'S UP TO END DEVICE that when it turns on, sends a request to coord to ask if there are pending msgs
2. coord sends an ack
3. if there're pending msgs will transmit the data
4. receiving ACK

- if no pending messages -> Coord responds that there aren't

DATA TRANSFER IN NON BEACON-ENABLED NETWORKS

Data transfer from a coordinator/router to an end device:

The coordinator stores the message and waits for the device to request for the data.

A device can poll the coordinator for pending messages by transmitting a Data request (using unslotted CSMA-CA)

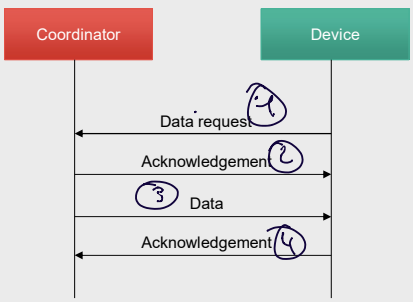
The coordinator send an ack for the request

The coordinator transmits the pending message(s) to the devices.

If no messages are pending, the coordinator transmits an empty message.

The device sends an ack

The coordinator discards the messages.



37

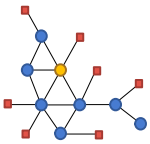
- [SO] THIS STANDARD is designed with the purpose to SAVE ENERGY AT MAC LAYER, this mechanism combines many things:
  1) SYNCHRONISATION: by using beacon and superframe structure
  2) ASYMMETRY BETWEEN FFD & RFD: to let RFD to save even more energy => to adopt very low DC, FFD low DC but beyond a certain point

& with P2P beacon enabled => no possible end → end

P2P with no SUPERFRAME

DATA TRANSFER IN NON BEACON-ENABLED NETWORKS

Peer-to-peer data transfers:



Each device may communicate with every other device in its radio range

The devices will need to remain always active or to synchronize with each other.

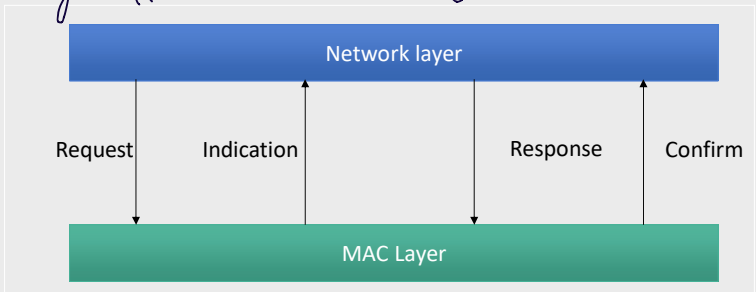
- In the first case the device can directly transmit the data
- In the latter case the devices synchronization is beyond the scope of the IEEE 802.15.4 standard (it is left to the upper layers)

- SERVICES OF MAC LAYER:
- implemented by: Request, Indication, Response, Confirm

38

MAC LAYER SERVICES: PRIMITIVES

- Difference with Zigbee: It uses Request and Confirm for the most of services
- Confirm in mac layer appears more frequently



39

- MAC layer offers:
  1) Data service
  2) Mgmnt service

send rec frame → sync notification frame OK/NOT → receive

R C I

The data service:

- implemented in term of data request: send data by net layer to mac layer → mac layer implements the request by the 4 protocols above

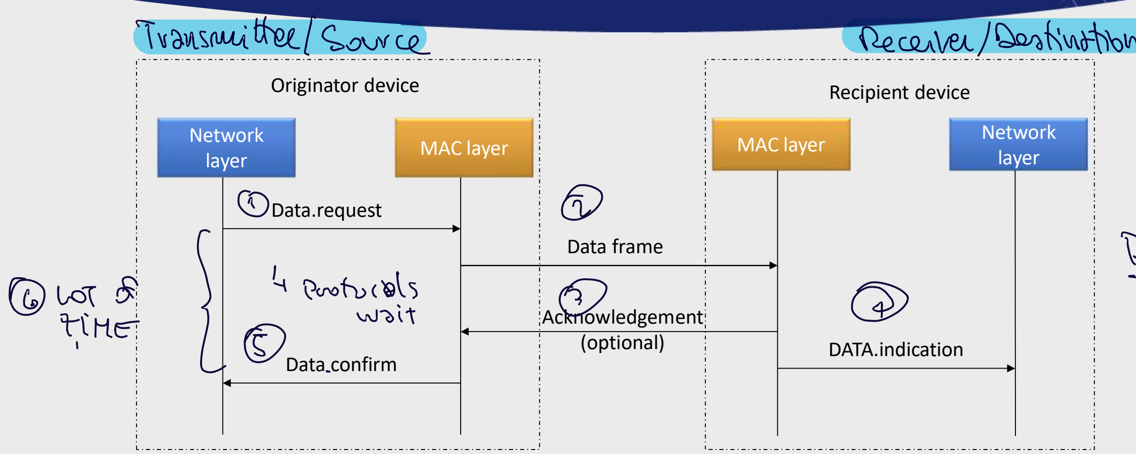
MAC LAYER DATA SERVICE

- Exploits only the request, confirm and indication primitives. NO RESPONSE
- DATA.request primitive: is invoked by the upper layer to send a message to another device.
- DATA.confirm primitive: reports the result of a transmission requested with a previous DATA.request primitive to the upper layer
  - Returns either success or an error code
- DATA.indication primitive: corresponds to a receive primitive: it is generated by the MAC layer on receipt of a message from the physical layer to pass the received message to the upper layer.

How it works:

- ① Network layer sends data via invoking: Data.req to MAC layer
- ② Mac layer sends the data frame using one of the 4 protocols seen before
- ③ May or not have an ack
- ④ When data frame is received to destination → network layer of destination receives an event of: DATA.indication (sort of an up call) ⇒ network layer is informed that a new frame has arrived.

MAC LAYER DATA SERVICE



DATA SERVICE: R.I.C.

⑤ At the TRANSMITTER, Mac layer informs the network layer with data.confirm that data has been sent
⇒ Data confirm may sent immediately after the data frame if no ack or if requested an ack
⇒ this data confirm is communicated to network layer after the ack

KEEP IN MIND: between the Data request (1) and Data confirm (5) you may spend a lot of time (6) cuz: you've to wait for the beacon, free slot, end device (devices) may be off... often some time, when the protocol for

transmitting a frame (before seen) is concluded, only at that time the mac layer will send Data.Confirm(S)

• MANGMNT SERVICES OF MAC LAYER

MAC LAYER MANAGEMENT SERVICE

Management services:

1) • PAN initialization: - when coord creates a net (in ZigBee) uses the MAC layer services to initialize the PAN and send the beacon
2) • Detection of existing PANs: - when you create a net, have to discover a free channel to allocate your net, or to join, have to discover the channel that are allocated, net ID, choose one, connect to it
3) • Devices association/disassociation: to an existing network: the join protocol of network layer however relies on an association protocol of a mac layer
4) • Other services . ..

• Services are implemented according to the request, indication, resp., conf.

42

O: OPTIONALLY
X: MANDATORY

Service to which MAC LAYER notifies to NTWRK layer that it has received a beacon from a coordinator
- In fact has only INDICATION which is receive
* providing the params in the beacon

→ req to coord time slots

→ cuz in ZigBee STNDRD they provide 2 WAYS to connect to an existing net:
- by its own will (endinitiate the connection)
- or coord forces a device to join to an existing network

MAC LAYER MANAGEMENT SERVICE

Name	Request	Indication	Response	Confirm	Functionality
ASSOCIATE	X	O	O	X	Request of association of a new device to an existing PAN.
DISASSOCIATE	X	X		X	Leave a PAN.
BEACON-NOTIFY		X			Provides to the upper layer the received beacon.
GET	X			X	Reads the parameters of the MAC.
GTS	O	O		O	Request of GTS to the coordinator.
SCAN	X			X	Look for for active PANs.
COMM-STATUS		X			Notify the upper layer about the status of a transaction that begun with a response primitive.
SET	X			X	Set parameters of the MAC layer.
START	O			O	Starts a PAN and begins sending beacons. Can also be used for device discovery.
POLL	X			X	Request for pending messages to the coordinator.

"O" means optional for RFDs

to an existing net. (ASSOCIATE)
SCAN: TO DISCOVER AN EXISTING NETWORK
START: w. the beacon
GET/SET: To read/set internal configuration of MAC layer

43

→ used by coord to tell to MAC layer: "from this point on start emitting the beacon" => O cuz used by coord/router, end not implement

→ POLL: req for pending msgs

ASSOCIATE

- Invocate by end device willing to join to an existing network
- implemented by invoking ASSOCIATE.REQUEST of end-device's mac layer
  => this invocation is implemented by the net layer and it's requested by the join service by network layer invoked by application layer
- To invoke an association.request the network layer should pass some parameters:
  1) channel to correct
  2) id of network

- During this protocol may be used the mac layer of the end device: cuz it has not living in the ntwk so have to communicate only the mac layer (MAC address)

ASSOCIATE PROTOCOL (END-DEVICE SIDE)

Is invoked by a device willing to associate with a PAN that has already been identified by a preliminary execution of the SCAN service (beacon-enabled networks)

The ASSOCIATE.request primitive takes as parameters (among others):

the PAN identifier,

the coordinator address,

the 64-bits extended IEEE address of the device,

It sends an association request message to the coordinator.

the association procedure is meant for beacon-enabled networks:

the association request message is sent during the CAP using the slotted CSMA-CA protocol.

The coordinator acknowledges the reception of the association messages

However, this acknowledgement does not mean that the request has been accepted...

44

- SO: - associate.request transmits a request to the coordinator and if coordinator accepts the request, it send back also the network address.
- the device will use this address both at the network layer and mac layer in all communication (save space in the header)
- THIS WAS THE JOIN PROTOCOL INVOKED BY APP LAYER OF ZIGBEE TO NETWORK LAYER

REMEMBER... THE JOIN PROTOCOL IN ZIGBEE...

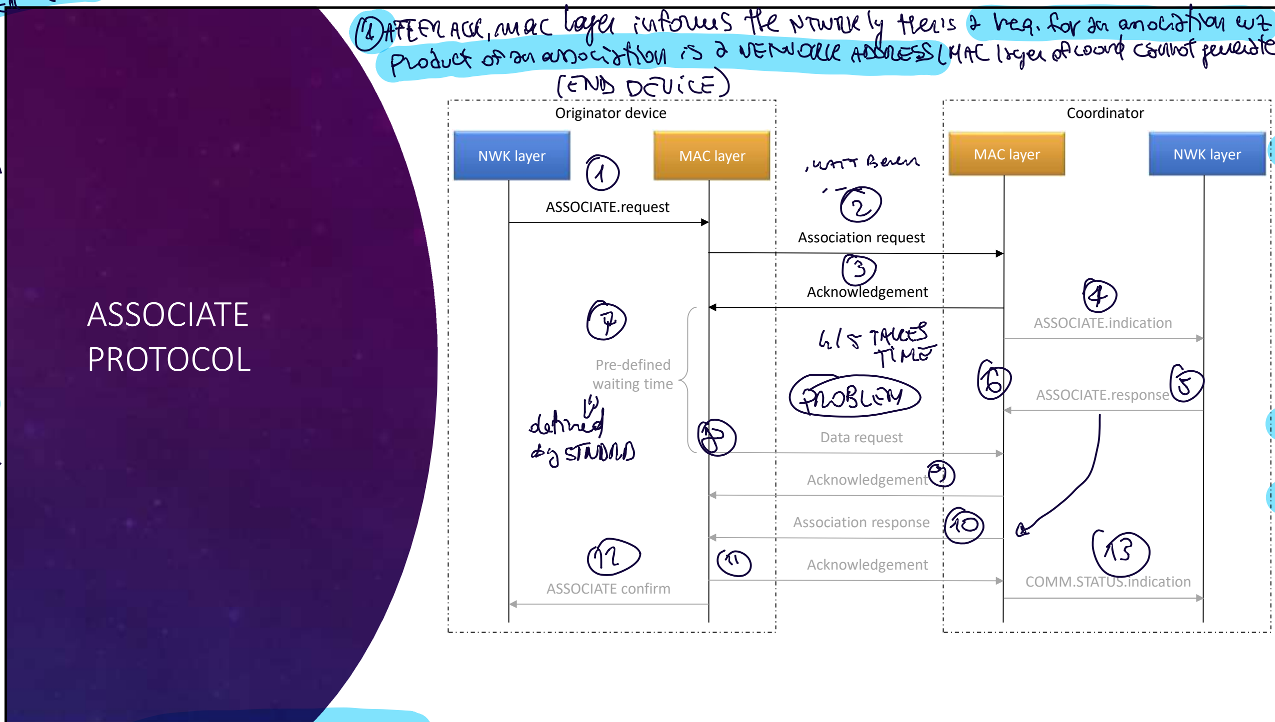
1) Network discovery requests for a scan at mac layer
1.B) Mac layer responds by give to ntwk layer list of active pans
3) NTWK gives this info to app layer
4) APP layer chooses one pan of a one channel
5) APP layer invokes join to NWK layer
6) Net layer invokes associate.req
7) Here, MAC layer implements the association protocol
8) Directly communicating with the coordinator of the network
9) Associate protocol ends with associate confirm providing to network layer 16-bits network address assigned to this end-device
10) Net layer uses a join.conf to APP layer informing the join is concluded

45

ASSOCIATE PROTOCOL: 1) NTWK layer invokes "associate.req": we already know which is the network => MAC layer already knows on which channel communicates and PAN address
2) MAC layer transmits a frame "associate.req" to MAC layer of coordinator: this is immediately ack (3) by coord and this request may be implemented with 1 of those mechanisms seen before (es. star beacon enabled, before sending this "association.req" MAC layer waits 4 the beacon, finds free contention slot, transmits the "associate.req" in this slot, => then ack by coord's MAC layer (3))

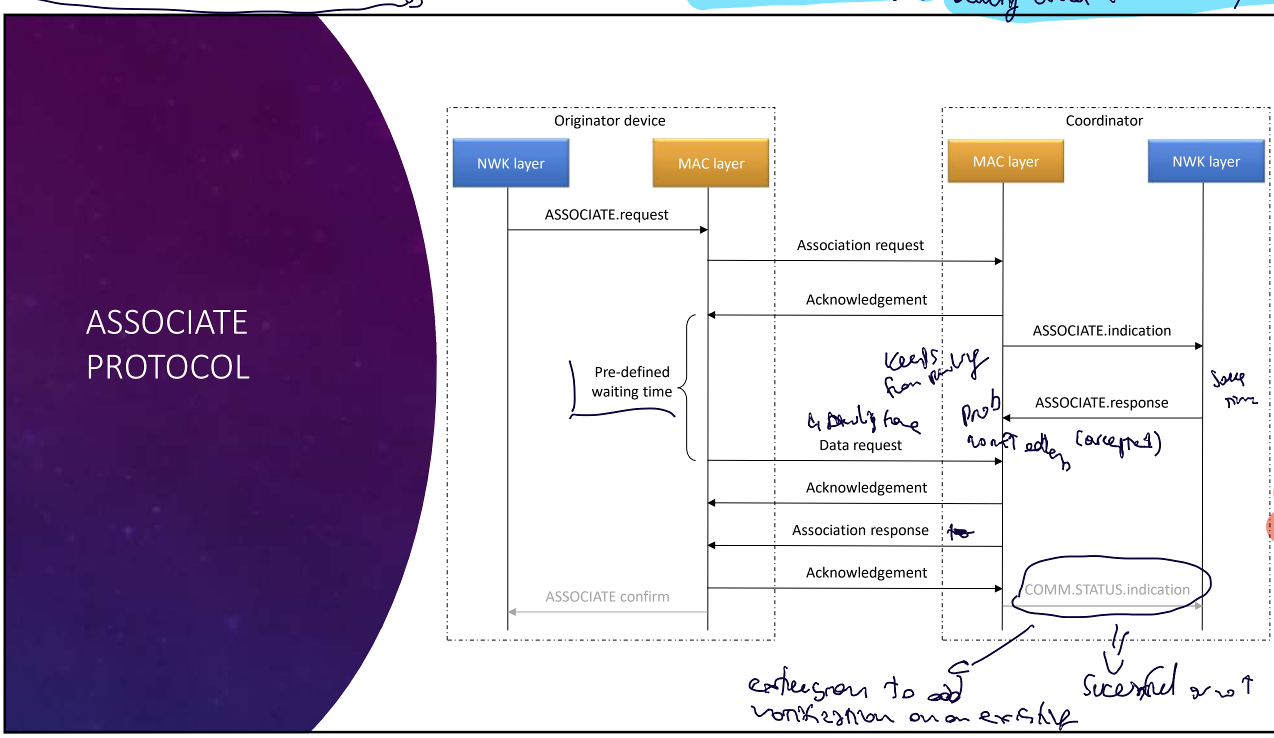
(7) On the end device is req. to associate, knows that the implementation of this operation from coord takes time (already estimated)
(8) After this time the end device sends a data request to req to MAC coord layer the pending frame
(9) Mandatory ack by coord
(10) Coord's MAC layer sends

(4) After ack, MAC layer informs the NTWK ly there's a req. for an association w/ product of an association is a NETWORK ADDRESS (MAC layer of coord cannot generate NTWK ADDRS) (END DEVICE)
(5) Confirms to MAC layer association is ok
(6) MAC layer has the response for this associate.req
PROBLEM: MAC layer can't transmit directly the response to the associate end device b/c end dev. isn't already part of network => no NTWK address
MAC layer keeps this frames of response for PENDING



46

the "association.response" (11) immediately ack
(12) At this point MAC ly sends to NTWK layer of the ED the "ASSOCIATE.confirm" to inform the association is successful / failed ⇓ also net address
(13) ALSO NET LAYER OF COORD IS INFORMED THE ASSOCIATION IS SUCCESSFUL b/c the net layer has allocated 1 network address for the end device (if fails can be reused) => COMM-STATUS.INDICATION is an extension to give the possibility of adding other notifications/commands to an existing service
no primitives to do this



extension to add notification on an existing; successful or not

NB: The network layer has obtained the MAC of end dev. and knows net address of the device => with this info will be passed to the application support sublayer (APS) that will update the address map used 4 binding

47

ASSOCIATE PROTOCOL (COORDINATOR SIDE)

The association request message is passed to the NWK layer (ASSOCIATION.indication)

- The NWK layer takes decides about the association

If the request is accepted, the NWK layer:

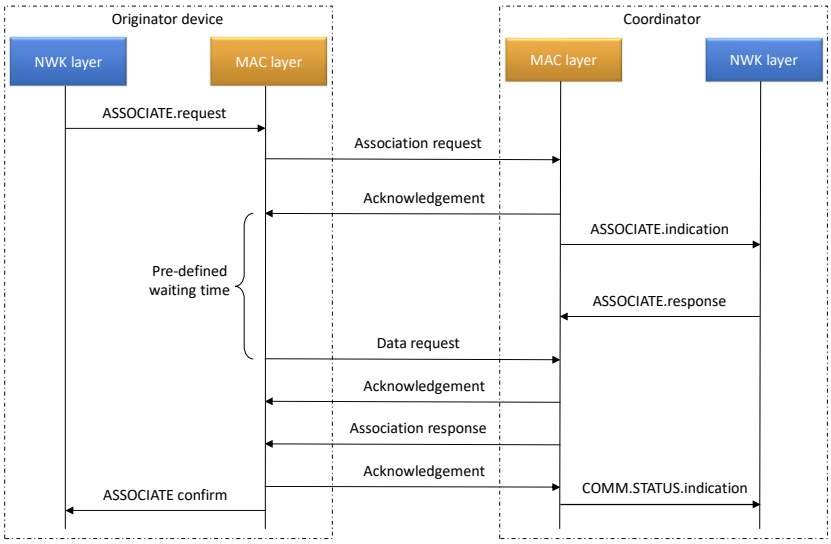
- **selects a short 16 bit address**
  - It will be used by the end-device in place of the 64-bit extended IEEE address.
- invokes the ASSOCIATE.response primitive
- This primitive takes as parameters the 64 bit address of the device, the new 16 bit short address and the status of the request.

The ASSOCIATE.response primitive:

- sends an association response command to the device
- The message is sent using indirect transmission

48

ASSOCIATE PROTOCOL



49

ASSOCIATE PROTOCOL

The MAC layer of the end-device:

- issues an ASSOCIATE.confirm primitive to the upper layer

The MAC layer of the coordinator:

- issues the COMM-STATUS.Indication primitive to the upper layer
  - To inform that the association is concluded
    - either with success or with an error code.

50

MAC LAYER SECURITY

The IEEE 802.15.4 MAC layers provides a basic support for security

- Advanced security features (such as keys management, device authentication) are left to the upper layers.
- The security features are optional and the applications can decide when and which functionality they use.

Security services based on symmetric-keys

- The keys are provided by the higher layers.

51

MAC LAYER SECURITY

Access control:

- each device maintains an Access Control List (ACL) of devices with whom it can communicate.
- frames received from devices not included in the ACL are discarded

Data encryption:

- symmetric encryption of data, commands and beacon payloads
- The encryption/decryption key:
  - can be shared by a group of devices (group key)
  - or it can be shared by only two peers (link key)

52

MAC LAYER SECURITY

Frame integrity:

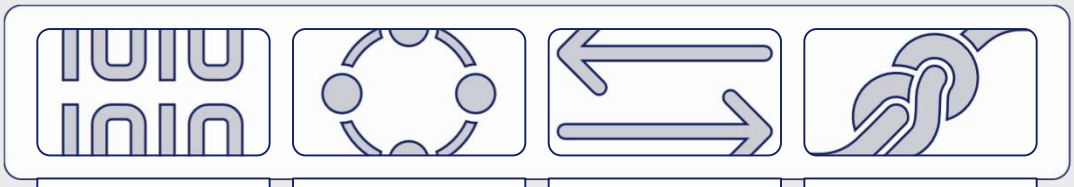
- Protects data, command and beacon frames from being altered by parties without the cryptographic key
  - assures that the data comes from a device with the cryptographic key.
- Integrity may be provided on data, beacon and command frames.
- Uses the same key used for encryption (either a group or a link key).

Sequential freshness:

- orders the sequence of input frames to ensure that an input frame is more recent than the last received frame.

53

SUMMARY



IEEE 802.15.4 standard: physical and MAC layers	Superframe	Modes of data transfer	Association of a device to a network

54