Reti ad Hoc & Reti di Sensori

The IEEE 802.15.4 and ZigBee standards

Stefano Chessa

Zigbee

- Standard for wireless sensor networks
  - Developed and promoted by the ZigBee alliance
- Applications:
  - Home automation (domotics, ambient assisted living,…)
  - Health care
  - Consumer electronics
  - Industrial control
  - …

Zigbee

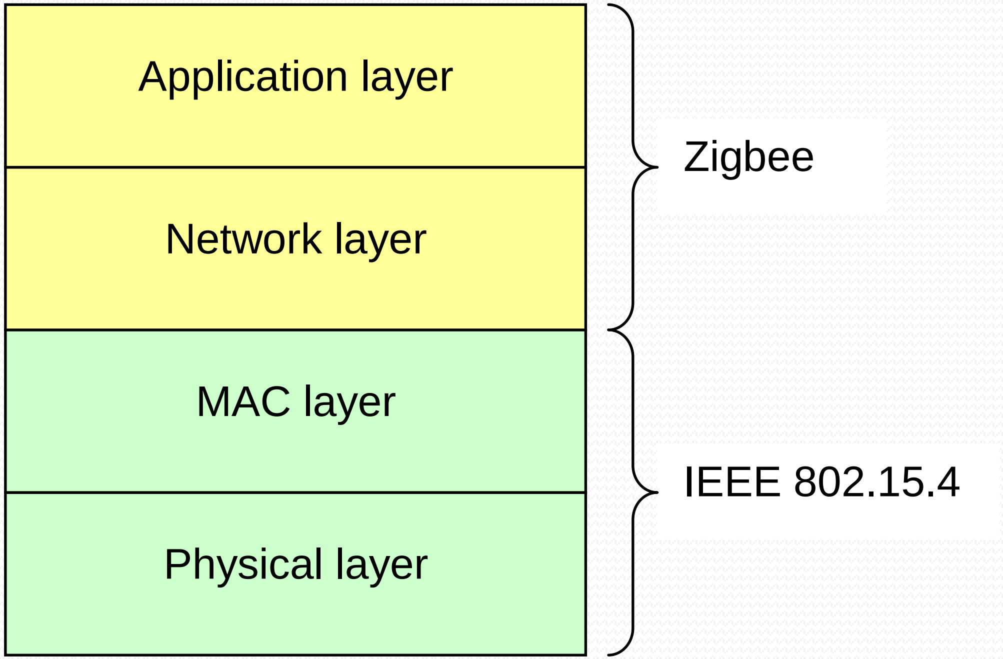
- Main requirements:
  - Network completely autonomous, no human intervention
  - Very long battery life
  - Low data rate
  - Interoperability of ZigBee devices from different vendors

Zigbee

- Main features:
  - Standards based
  - Low cost
  - Can be used globally
  - Reliable and self healing
  - Supports large number of nodes
  - Easy to deploy
  - Very long battery life
  - Secure

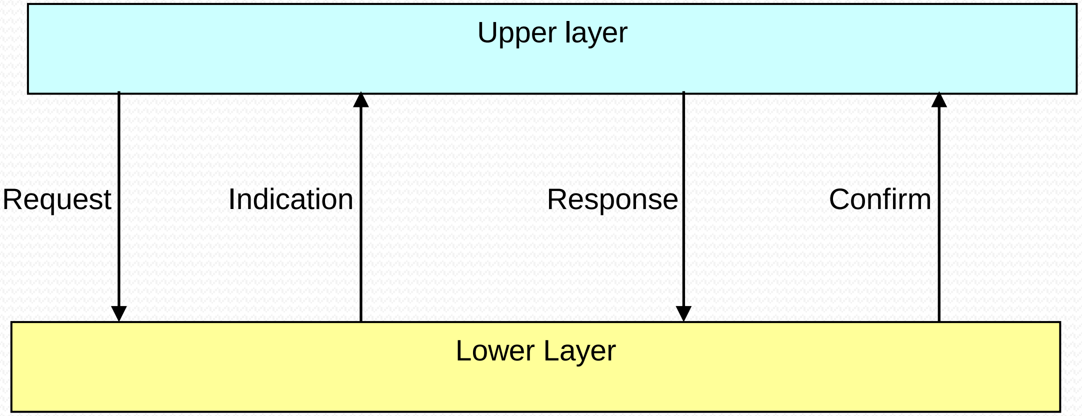
IEEE 802.15.4 & Zigbee

- IEEE 802.15.4 first delivered in 2003 and revised in 2006
  - The first revision of the standard is freely distributed
- ZigBee first delivered at the end of 2004, revised in 2006
  - Proposed by the ZigBee Alliance, an association of companies
  - The first revision of the standard is freely distributed

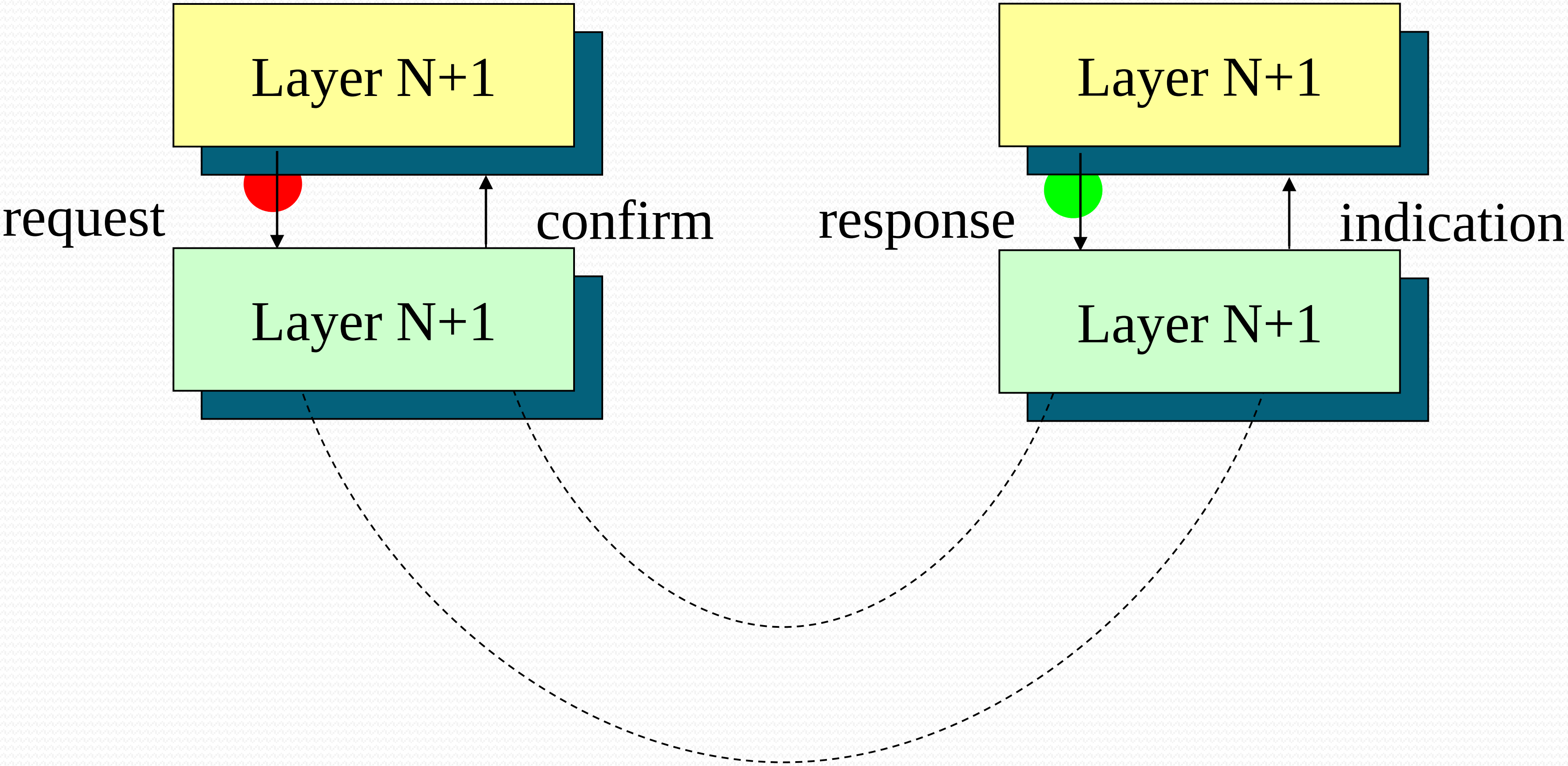


Service primitives

- Each layer provide s its data and management services to the upper layer
- Each service is specified by a set of primitives which can be of four generic types:
  - **Request**: It is invoked by the upper layer to request for a specific service;
  - **Indication**: It is generated by the lower layer and is directed to the upper layer to notify the occurrence of an event related to a specific service;
  - **Response:** It is invoked by the upper layer to complete a procedure previously initiated by an indication primitive;
  - **Confirm:** It is generated by the lower layer and is directed to the upper layer to convey the results of one or more associated previous service requests.
- Each service may use all or part of the four primitives depending on its needs



Service primitives



Part I

The IEEE 802.15.4 standard

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:

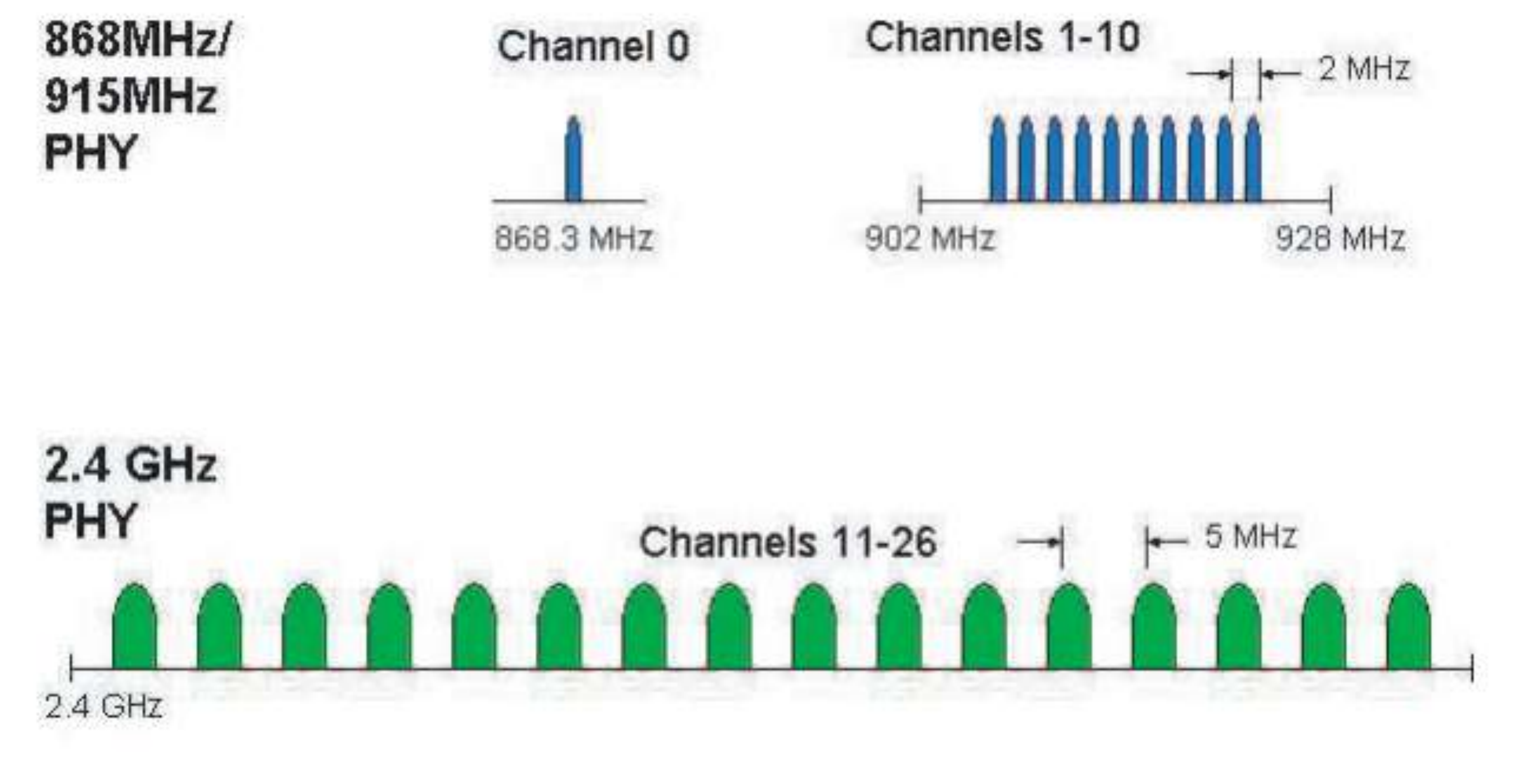
- Can coexist with IEEE 802.11 and IEEE 802.15.1 (Bluetooth),…
- Licence free frequency bands:
  - 868–868.6 MHz (e.g., Europe) with a data rate of 20 kbps;
  - 902–928 MHz (e.g., North America) with a data rate of 40 kbps; or
  - 2400–2483.5 MHz (worldwide) with a data rate of 250 kbps.

Physical layer

Physical layer

- Data Service
  - Transmission/Reception of *PHY Protocol Data Unit* (PPDU) through the physical medium.
- Management Service
  - Radio transceiver activation/desactivation
  - Energy Detection - ED)
  - Link Quality Indicator – LQI
  - Channel Selection
  - Clear Chanel Assessment – CCA
  - PHY-PIB (PHY PAN Information Base) Configuration

Physical layer

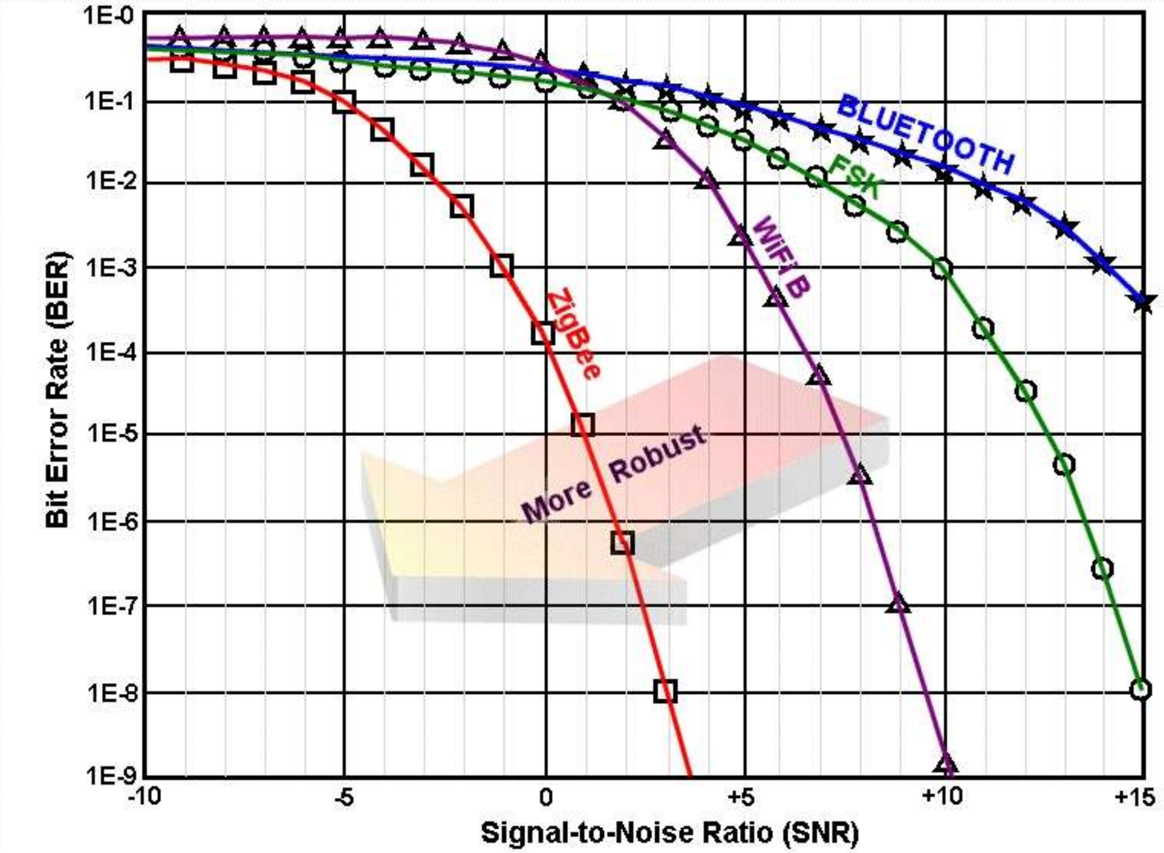


Physical layer: example

- Frequency band: 868-868.6 MHz
- Modulation: BPSK (Binary Phase Shift Keying)
- bit rate: 20 kbps
- Symbols: binary
- 1 channel centered on 868.3 MHz
- Maximum packet size (bytes): 127

Physical layer: performance

- excellent performance in low SNR environments



Physical layer: energy detection

- Estimation time for ED = average over 8 symbol intervals
- Detection threshold at 10dB above the sensitivity level
- ED result given in a byte
- ED level range is at least 40dB

Physical layer: link quality indicator

- Link Quality Indicator (LQI) indicates the quality of data packets that are received by a node.
- LQI is based on ED, or on the signal/noise ratio, or both.
- LQI is assessed each time a packet is recepted.
- LQI must have at least 8 different levels.
- The estimated value for LQI is forwarded to the network and application layers.

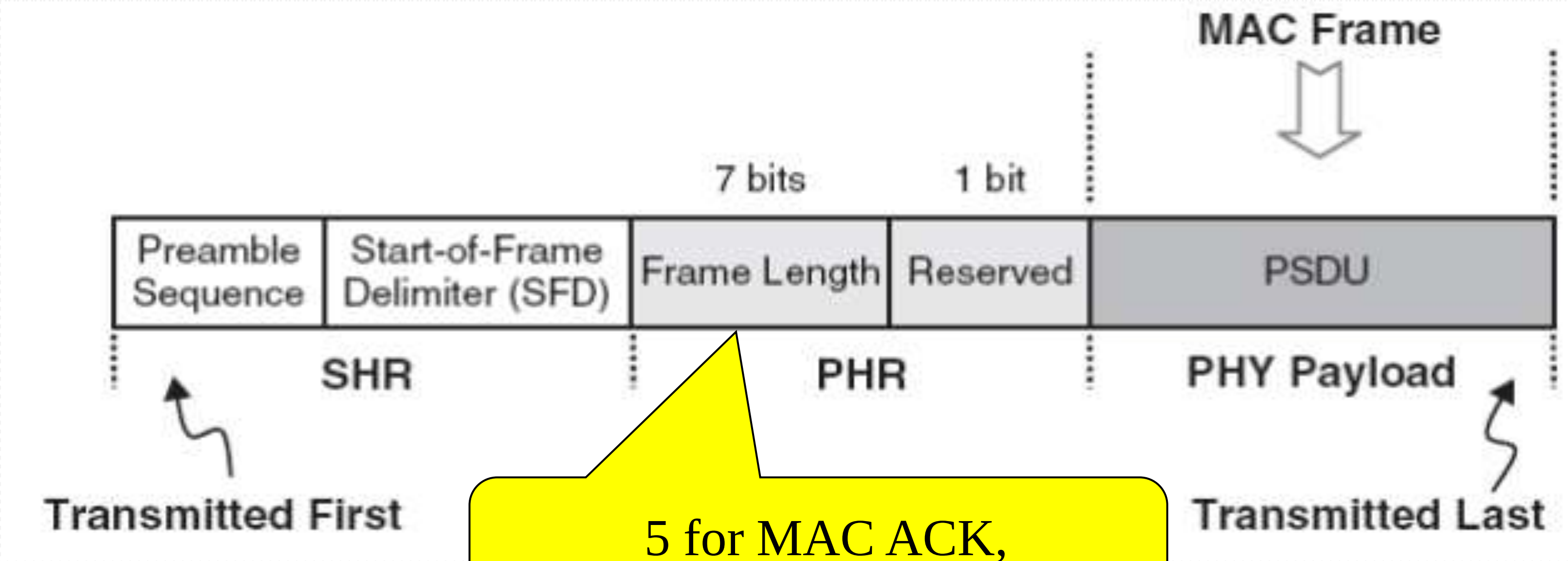
Physical layer: channel assessment

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

Physical layer: data services

- In the MAC layer: MPDU (MAC Protocol Data Unit)
- PPDU (PHY PDU) reports the result of the process to the upper layer (success or fail)
- The reason that the emission fails can be:
  - radio transceiver out of order
  - radio transceiver is in the reception mode
  - radio transceiver busy

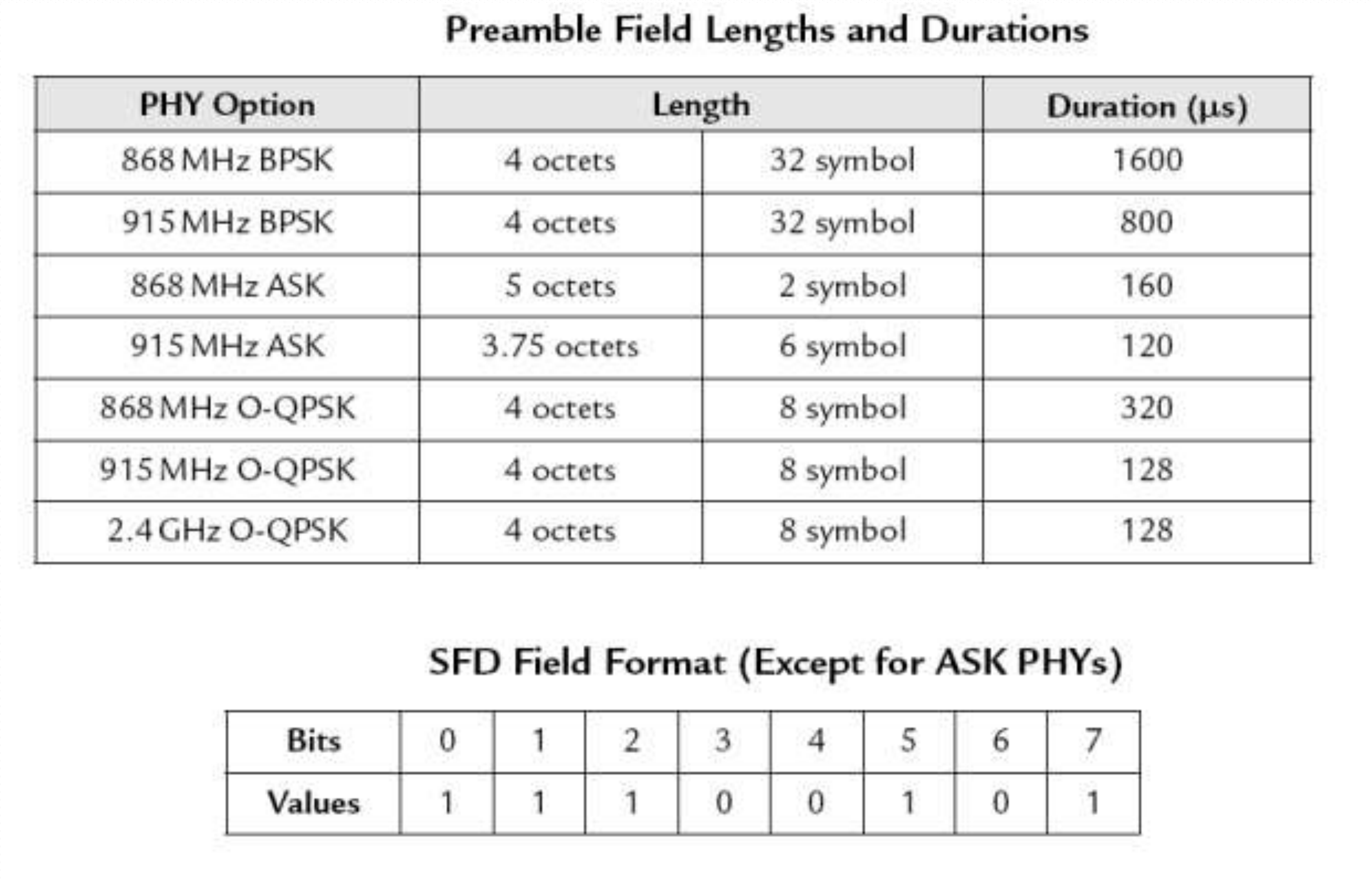
Physical layer: the frame



5 for MAC ACK,
9-127 for other packet types

- SHR (Synchronization Header):
  - synchronisation with the receiver
- PHR (PHY Header): information about the frame length
- PHY Payload: the MAC frame

Physical layer: the frame



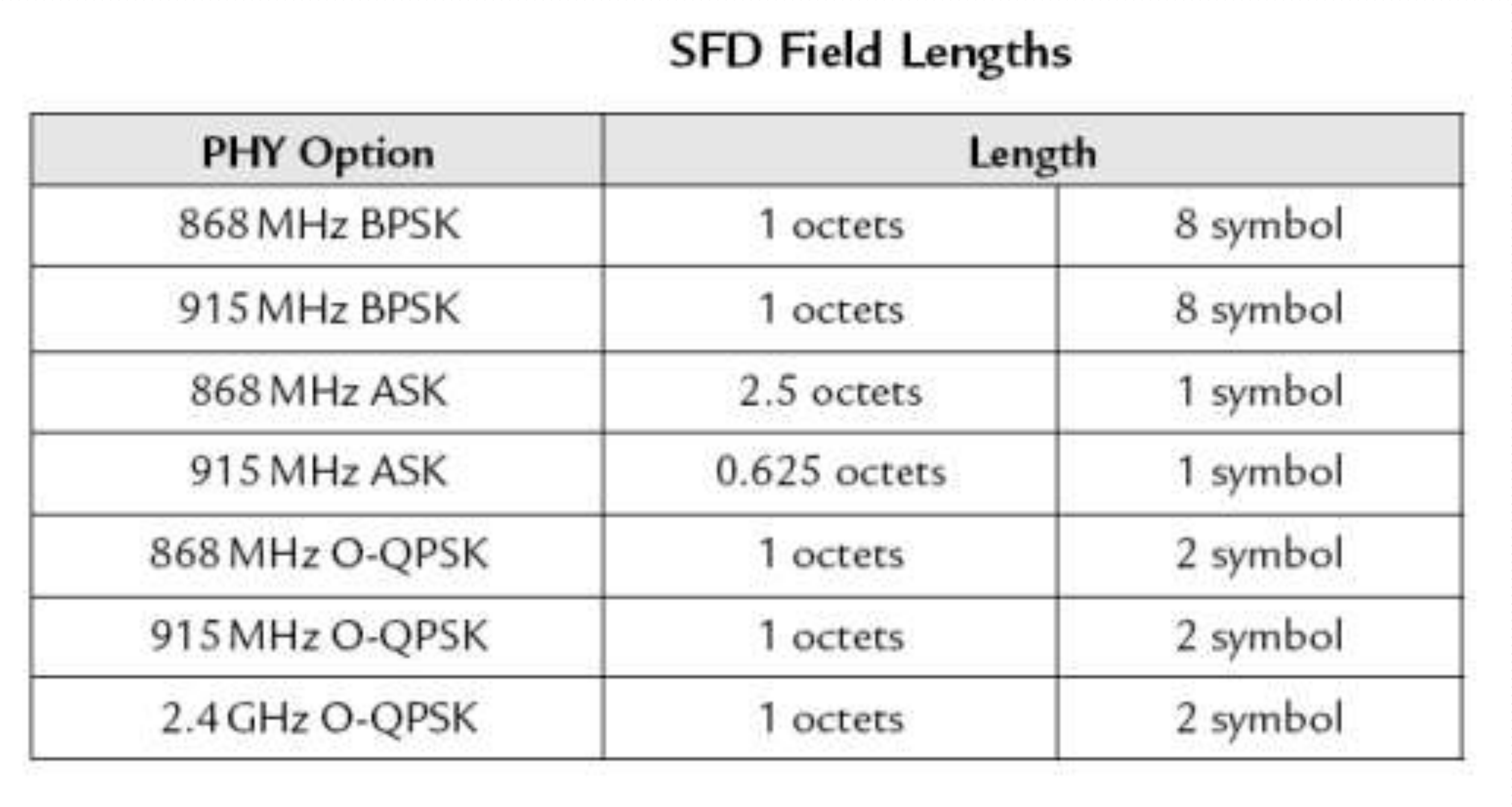
Preamble Field Lengths and Durations

PHY Option	Length		Duration (µs)
868 MHz BPSK	4 octets	32 symbol	1600
915 MHz BPSK	4 octets	32 symbol	800
868 MHz ASK	5 octets	2 symbol	160
915 MHz ASK	3.75 octets	6 symbol	120
868 MHz O-QPSK	4 octets	8 symbol	320
915 MHz O-QPSK	4 octets	8 symbol	128
2.4 GHz O-QPSK	4 octets	8 symbol	128

SFD Field Format (Except for ASK PHYs)

Bits	0	1	2	3	4	5	6	7
Values	1	1	1	0	0	1	0	1

Physical layer: the frame



SFD Field Lengths

PHY Option	Length	
868 MHz BPSK	1 octets	8 symbol
915 MHz BPSK	1 octets	8 symbol
868 MHz ASK	2.5 octets	1 symbol
915 MHz ASK	0.625 octets	1 symbol
868 MHz O-QPSK	1 octets	2 symbol
915 MHz O-QPSK	1 octets	2 symbol
2.4 GHz O-QPSK	1 octets	2 symbol

MAC layer

MAC layer

The MAC layer services:

- Data services
  - transmission and reception of MAC packets across the physical layer.
- Management services
  - synchronization of the communications,
  - channel access,
  - management of guaranteed time slots,
  - association and disassociation of devices to the network.
- Security mechanisms

MAC layer

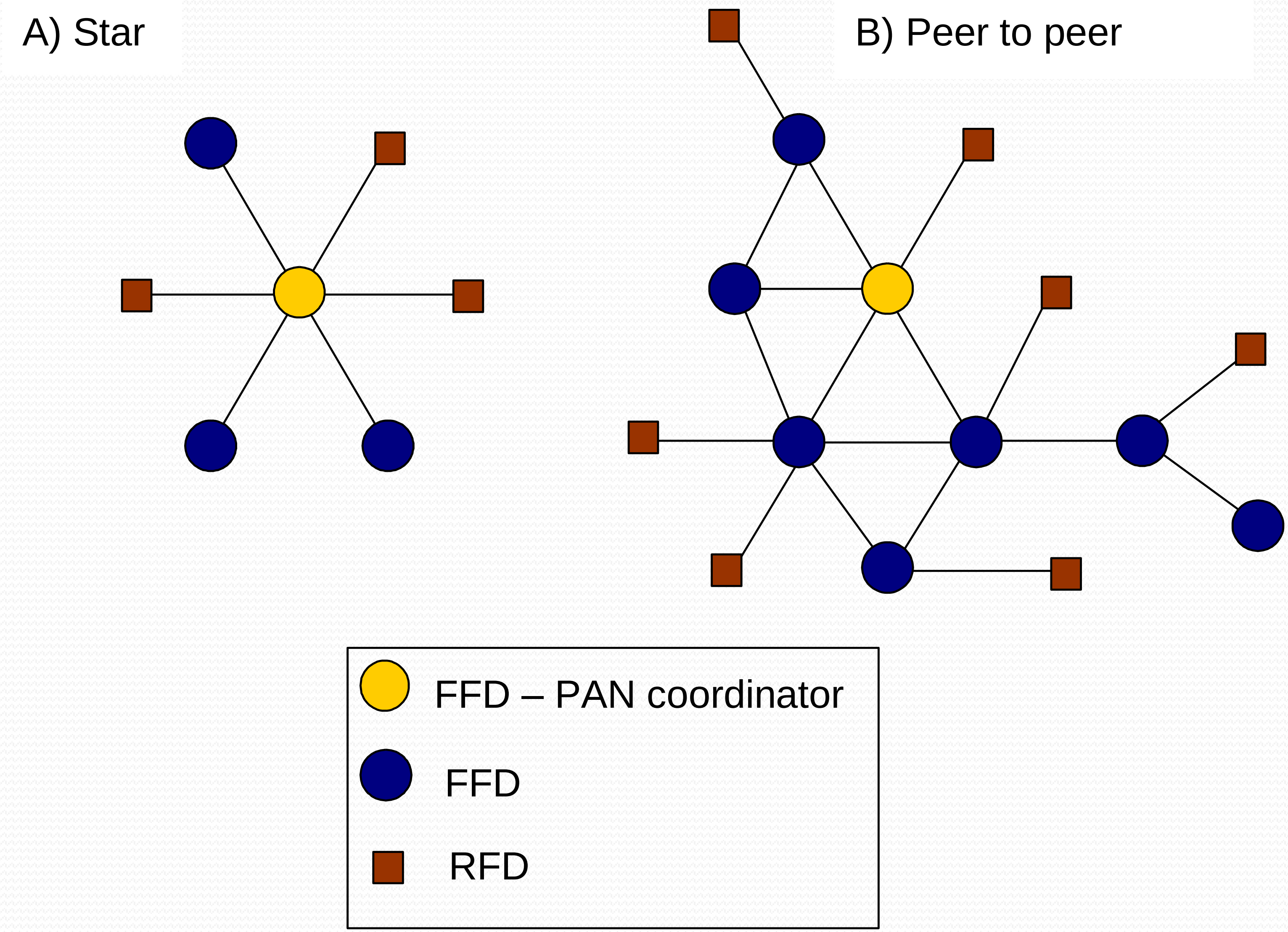
Two types of nodes:

- Reduced Function Devices (RFDs)
  - end-devices with reduced processing, memory, and communication capabilities which
    - simple sensors or actuators like light switches, lamps and similar devices.
  - implement a reduced set of functions of the MAC layer.
    - Join to an existing network
    - RFD depend on FFDs for communication.
    - One RFD can be associated to only one FFD at a time.
- 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
    - It selects the PAN identifier
    - manages associations or disassociation of devices.

MAC layer: topologies

- Topology implemented at the network layer by the FFD
- Star
  - One FFD is the PAN coordinator; the other nodes behave as RFDs
  - The PAN coordinator synchronizes all the communications in the network.
  - Different stars have different PAN identifier and are independent
- Peer to peer
  - Each FFD communicate with any other device within its radio range
  - One FFD is the PAN coordinator; the other FFD are routers
  - Each RFD acts as an end device and it is connected with one FFD

MAC layer: topologies



A) Star

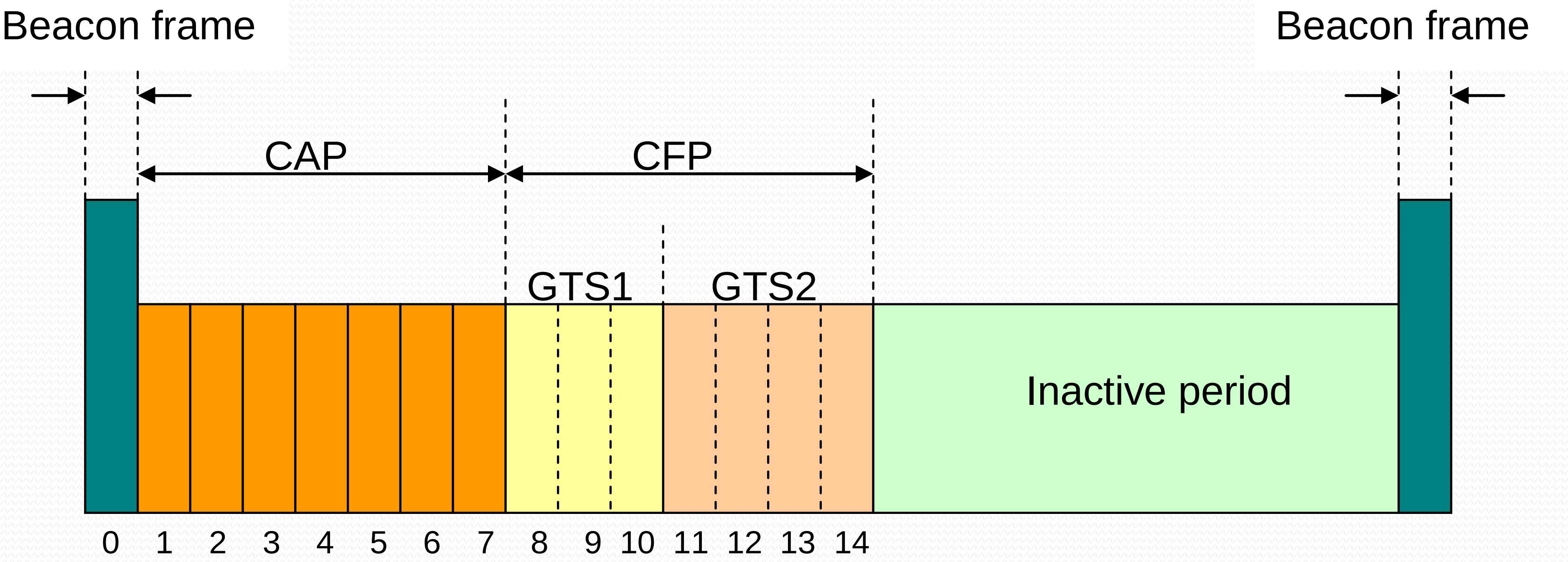
B) Peer to peer

- 🟡 FFD – PAN coordinator
- 🔵 FFD
- 🟫 RFD

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
  - provides synchronization between nodes
    - enable power savings of the devices.
- without a superframe structure.
  - is more general
  - used to support communications in arbitrary peer to peer topologies

Channel access with superframe



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.
  - The time slots are equally sized
  - The first time slots is the beacon frame and is sent by the PAN coordinator to begin the superframe.
  - The beacons are used to:
    - Synchronize the attached devices,
    - identify the PAN,
    - describe the structure of the superframes.
  - The actual communications between the end devices and the coordinator take place in the remaining time slots.

Channel access with superframe

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

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 wishing to transmit shall locate the boundary of the next slot and then wait for a random number of slots. If the channel is busy the device shall wait for another random number of slots before trying to access the channel again. If the channel is idle, the device can begin transmitting on the next available slot.
  - Objective: gain access to the medium (CSMA-CA) once the transmission has started, the node keeps the medium until the end of the frame

Channel access with superframe

- The CFP period:
  - Is optional
  - Is used for low-latency applications or applications requiring specific data bandwidth.
  - Occupies the last time slots of the active period
  - It is divided in Guaranteed Time Slots or GTS
    - Each GTS assigned by the PAN coordinator to a specific application
    - The application access 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 TS)

Channel access with superframe

- The CFP cannot 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 complete before the CFP.
  - Each device transmitting in a GTS shall complete the transmission within its GTS.

Channel access with superframe

- Any coordinator may send beacons and create its own superframes.
- Active periods of two superframes must be equal
- The coordinator creating a superframe send only a beacon starting the superframe.
- All routers in the same network use the same parameters for the beacon and superframe length

InterFrame Spacing – IFS

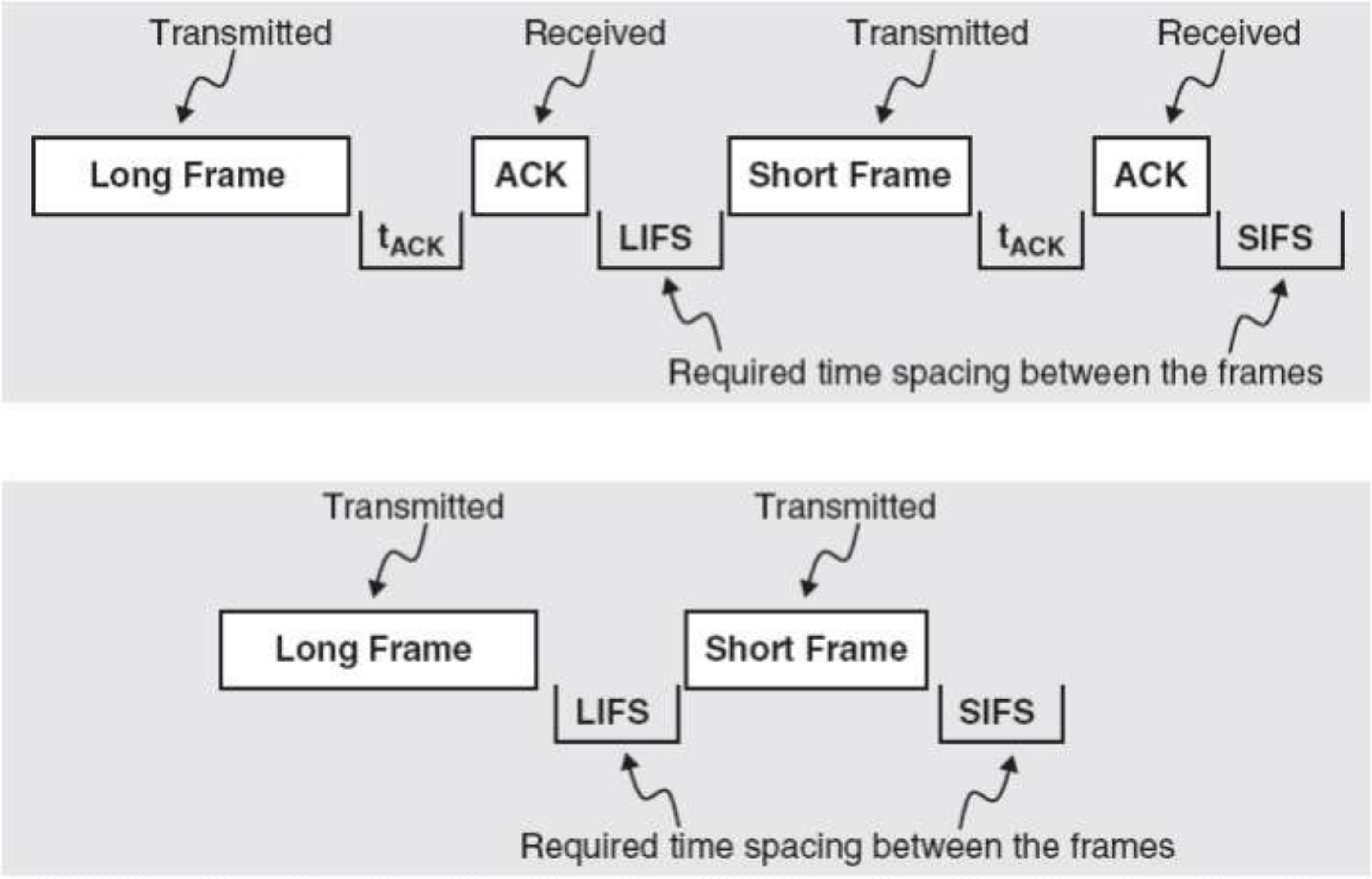
- The sender must wait a minimal time interval between two successive emissions: InterFrame Spacing (IFS)
- IFS size depends on the previous packet size
  - After a wide frame there must be a long IFS

    macMinLIFSPeriod = 40 symbols
  - After a short frame, there is a short IFS

    macMinSIFSPeriod = 12 symbols

- The distance between a data packet emission and reception of its ACK is t_{ACK}

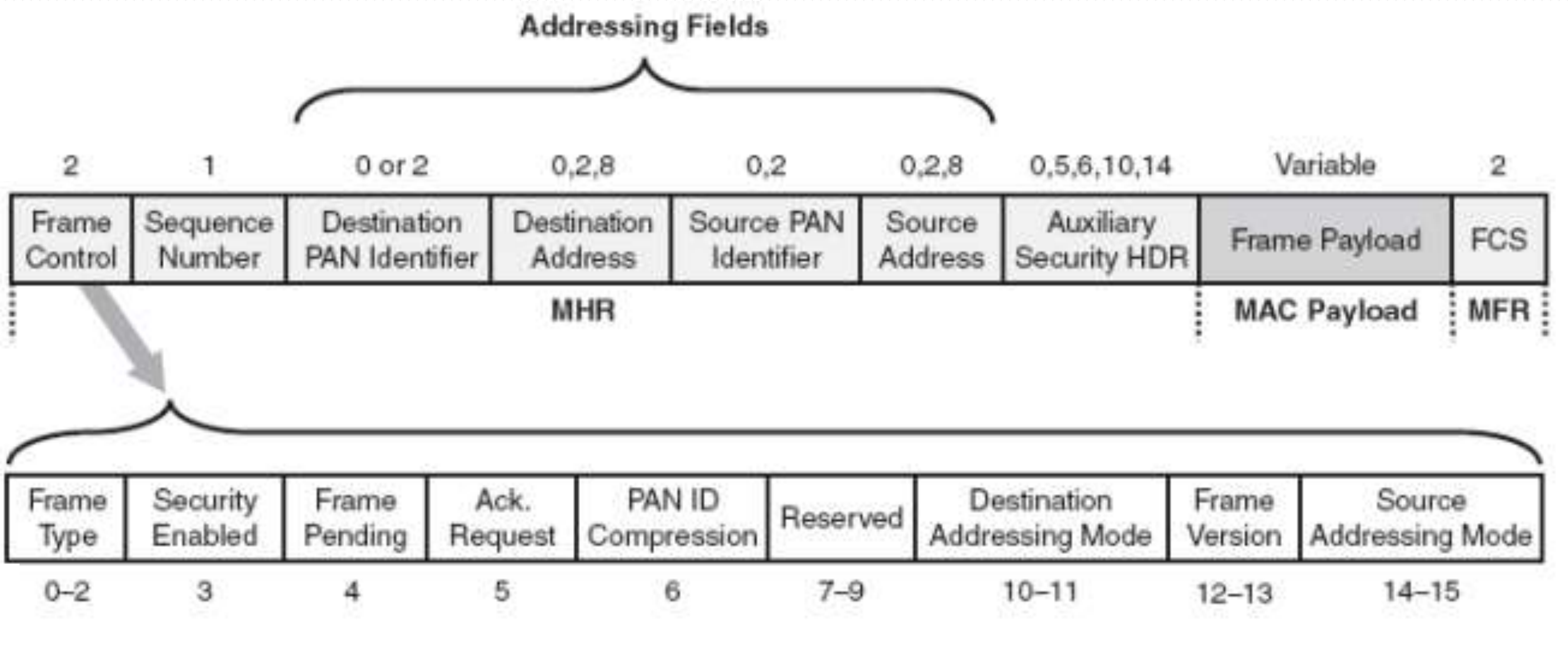
InterFrame Spacing – IFS



Frame types

- 4 frame types:
  - Beacon frame
  - Data frame
  - Acknowledgement frame
  - Command frame (MAC)

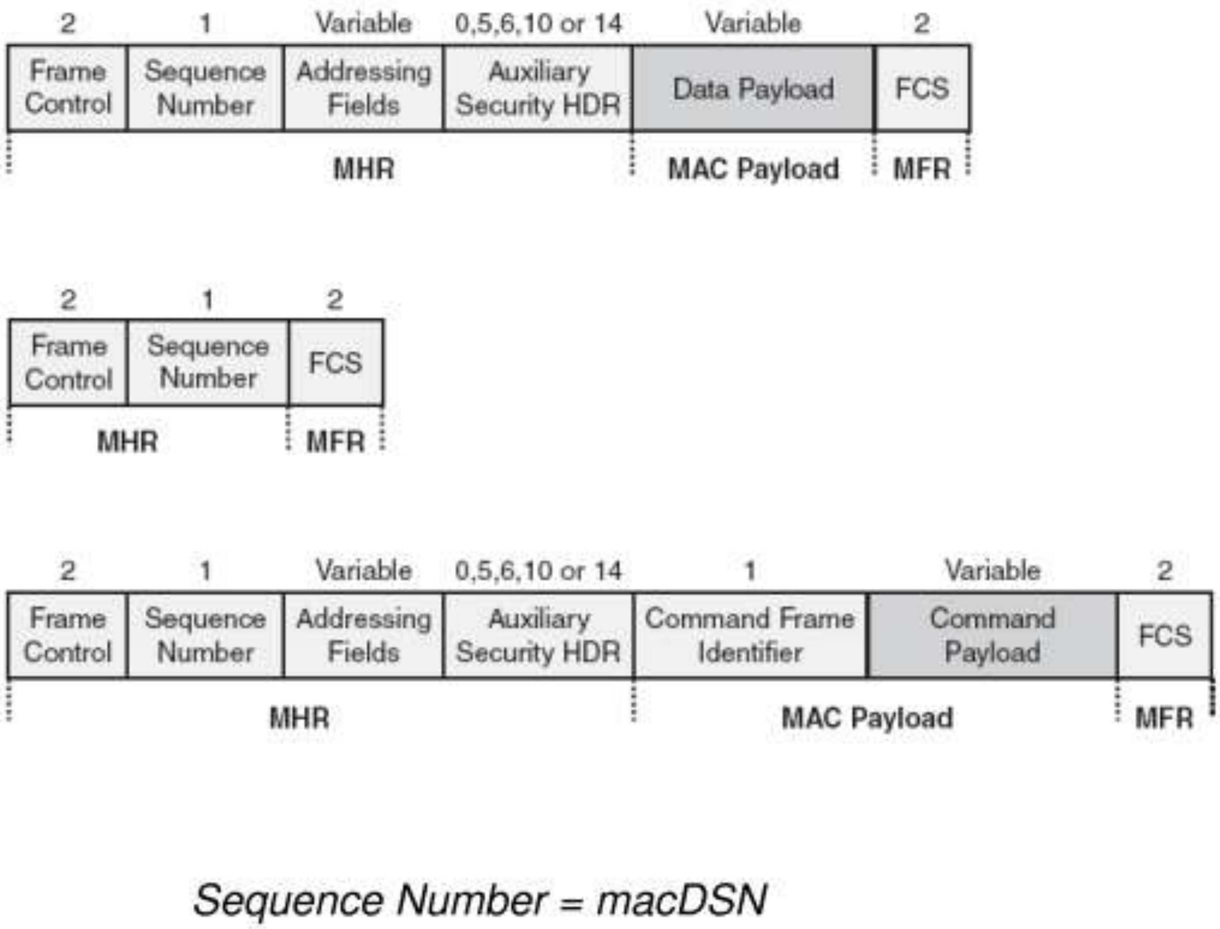
General frame format



			Addressing Fields						
bytes	2	1	0 or 2	0,2,8	0,2	0,2,8	0,5,6,10,14	Variable	2
	Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security HDR	Frame Payload	FCS
	MHR							MAC Payload	MFR

	Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	Reserved	Destination Addressing Mode	Frame Version	Source Addressing Mode
bits	0–2	3	4	5	6	7–9	10–11	12–13	14–15

Data, ACK and command frames



Data frame

bytes	2	1	Variable	0,5,6,10 or 14	Variable	2
	Frame Control	Sequence Number	Addressing Fields	Auxiliary Security HDR	Data Payload	FCS
	MHR				MAC Payload	MFR

ACK frame

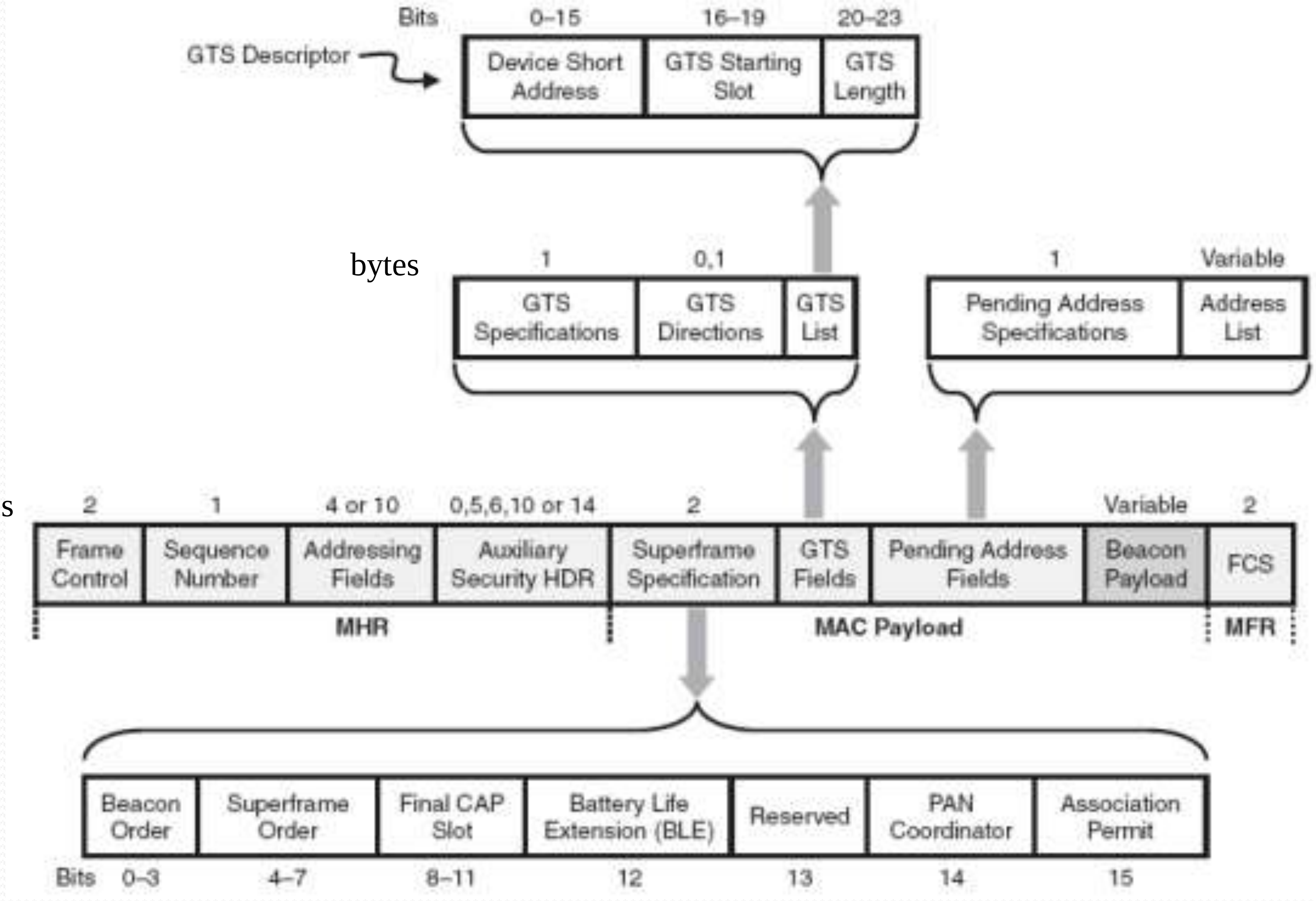
bytes	2	1	2
	Frame Control	Sequence Number	FCS
	MHR		MFR

Command frame

bytes	2	1	Variable	0,5,6,10 or 14	1	Variable	2
	Frame Control	Sequence Number	Addressing Fields	Auxiliary Security HDR	Command Frame Identifier	Command Payload	FCS
	MHR				MAC Payload		MFR

Sequence Number = macDSN

Beacon frames



GTS Descriptor

Bits	0–15	16–19	20–23
	Device Short Address	GTS Starting Slot	GTS Length

bytes	1	0,1	
	GTS Specifications	GTS Directions	GTS List

1	Variable
Pending Address Specifications	Address List

bytes	2	1	4 or 10	0,5,6,10 or 14	2			Variable	2
	Frame Control	Sequence Number	Addressing Fields	Auxiliary Security HDR	Superframe Specification	GTS Fields	Pending Address Fields	Beacon Payload	FCS
	MHR				MAC Payload				MFR

Bits	0–3	4–7	8–11	12	13	14	15
	Beacon Order	Superframe Order	Final CAP Slot	Battery Life Extension (BLE)	Reserved	PAN Coordinator	Association Permit

Channel access without superframe

- The PAN coordinator may optionally avoid the use of the superframe structure
  - The PAN is called *non beacon-enabled*
- The PAN coordinator never sends beacons
- Communication based on the unslotted CSMA-CA protocol.
- The coordinators (PAN coordinator and routers) are always on and ready to receive data from an end-device
- 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 sends these messages or signals that none is available.

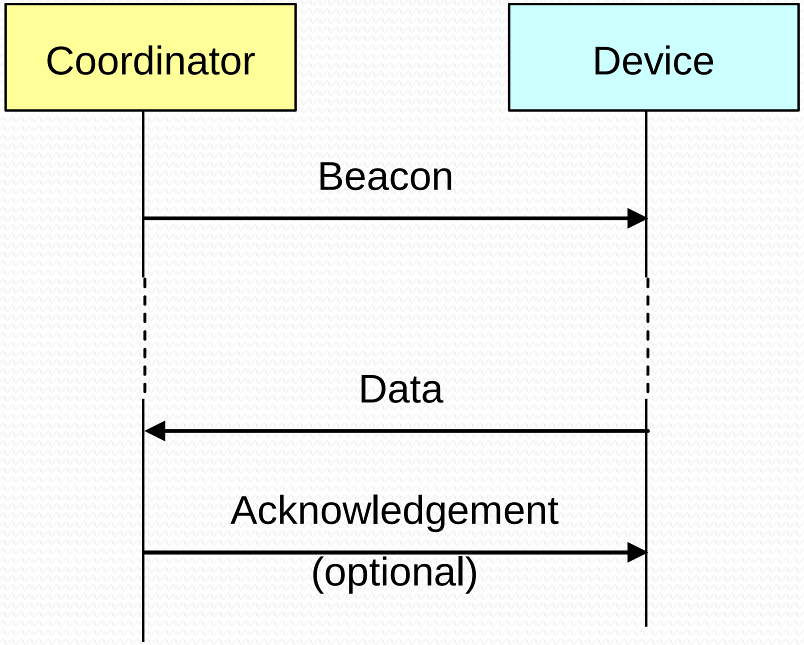
Data transfer modes

- Three types of data transfer:
  1. End device to coordinator
  2. Coordinator to end device
  3. Peer to peer.
- The star topology use 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.
- The implementation of these models depends on whether the network supports the transmission of beacons.

Data transfer in beacon enabled networks

Data transfer from an end device to a coordinator :

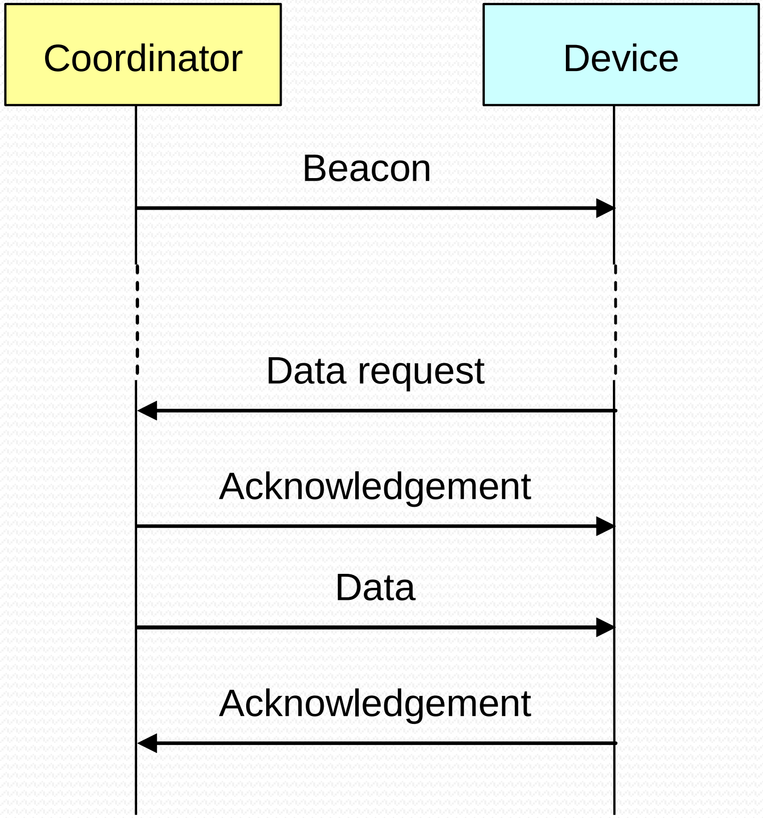
- The end device first waits for the network beacon to synchronize with the superframe.
- If it owns a GTS it directly use it
- Else it transmits the data frame to the coordinator using the slotted CSMA-CA protocol in one of the frames in the CAP period.
- The coordinator may optionally send an acknowledgement



Data transfer in beacon enabled networks

Data transfer from a coordinator to an end device :

- The coordinator stores the message and it indicates in the network beacon that the data message is pending.
- The end-device usually sleeps most of the time and it periodically listens to the network beacon to check for pending messages.
- When it notice that a message is pending it explicitly requests the message to the coordinator in the CAP period.
- The coordinator sends the pending message in the CAP period.
- The device sends an acknowledgment frame in a successive time slot
- The coordinator removes the pending message from its list.



Data transfer in beacon enabled networks

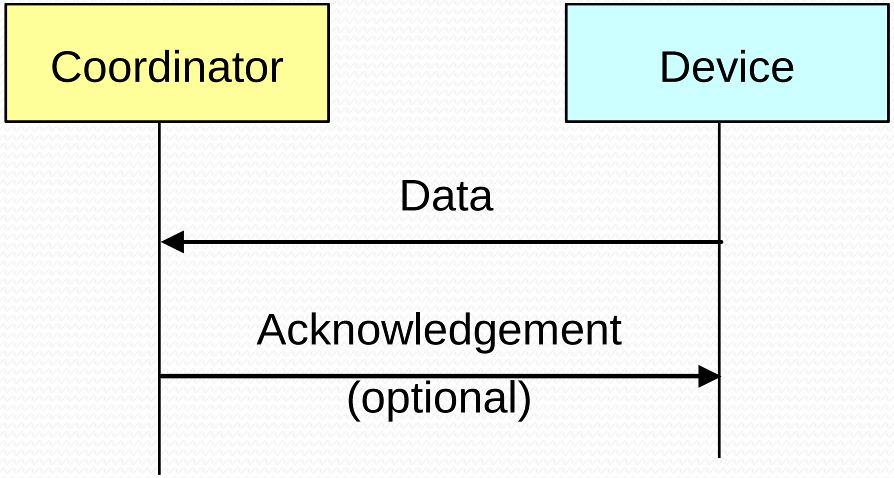
Peer-to-peer data transfers :

- If the sender or the receiver is a end device then one of the above schemes is used.
- If the sender and the destination are coordinators:
  - 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.

Data transfer in non beacon-enabled networks

Data transfer from an end device to a coordinator :

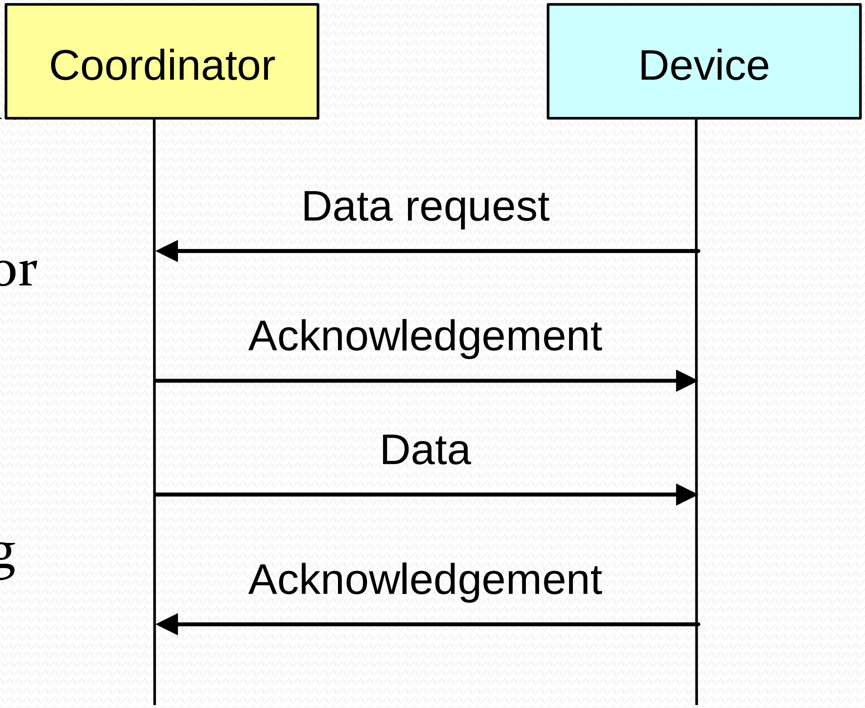
- the end device simply transmits its data frame to the coordinator using unslotted CSMA-CA.
- The coordinator acknowledges the successful reception of the data by transmitting an optional acknowledgment frame.



Data transfer in non beacon-enabled networks

Data transfer from a coordinator to an end device :

- The coordinator stores the message an waits for the device to request for the data.
- A device can inquiry the coordinator for pending messages by transmitting a request (using unslotted CSMA-CA)
- The coordinator send an ack for the request
- The coordinator transmits the pending messages to the devices.
  - If no messages are pending, the coordinator transmits an empty message.
- The device sends an ack
- The coordinator can discard the pending messages.

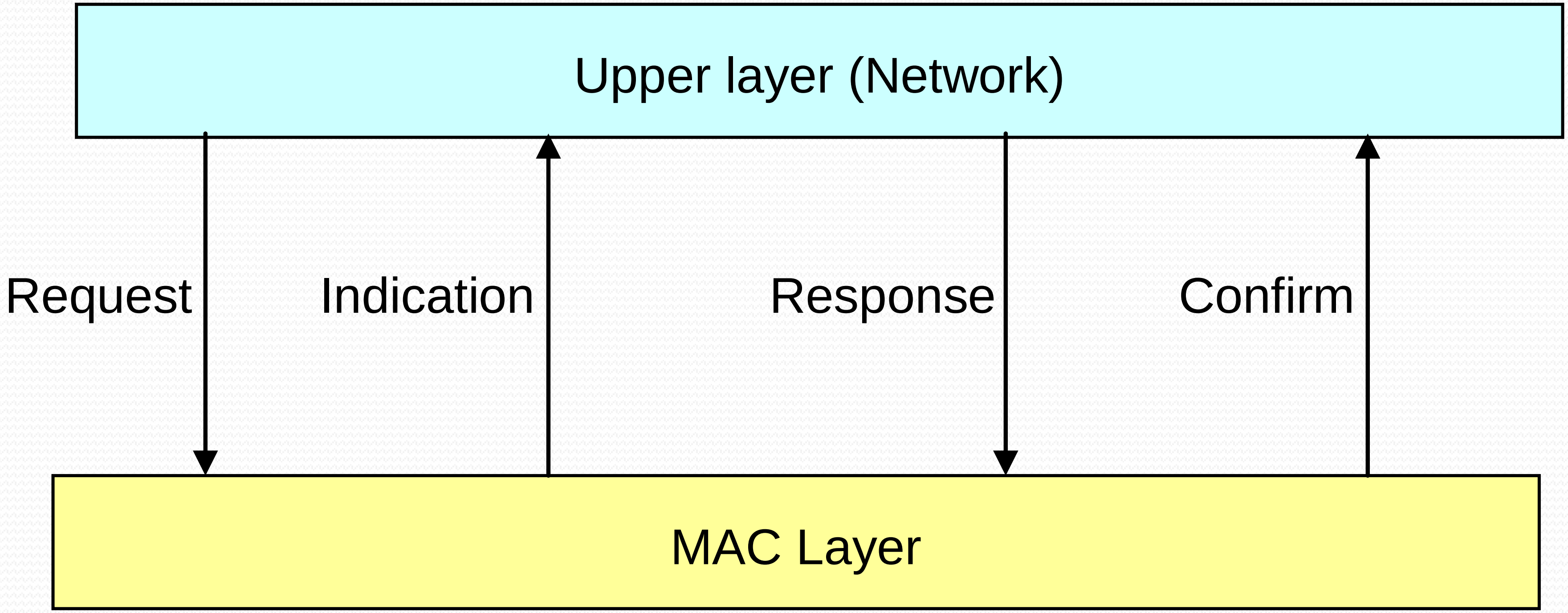


Data transfer in non beacon-enabled networks

Peer-to-peer data transfers :

- Each device may communicate with every other device in its radio range
- The devices wishing to communicate will need to either receive constantly or synchronize with each other.
  - In the former 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)

MAC layer services: primitives

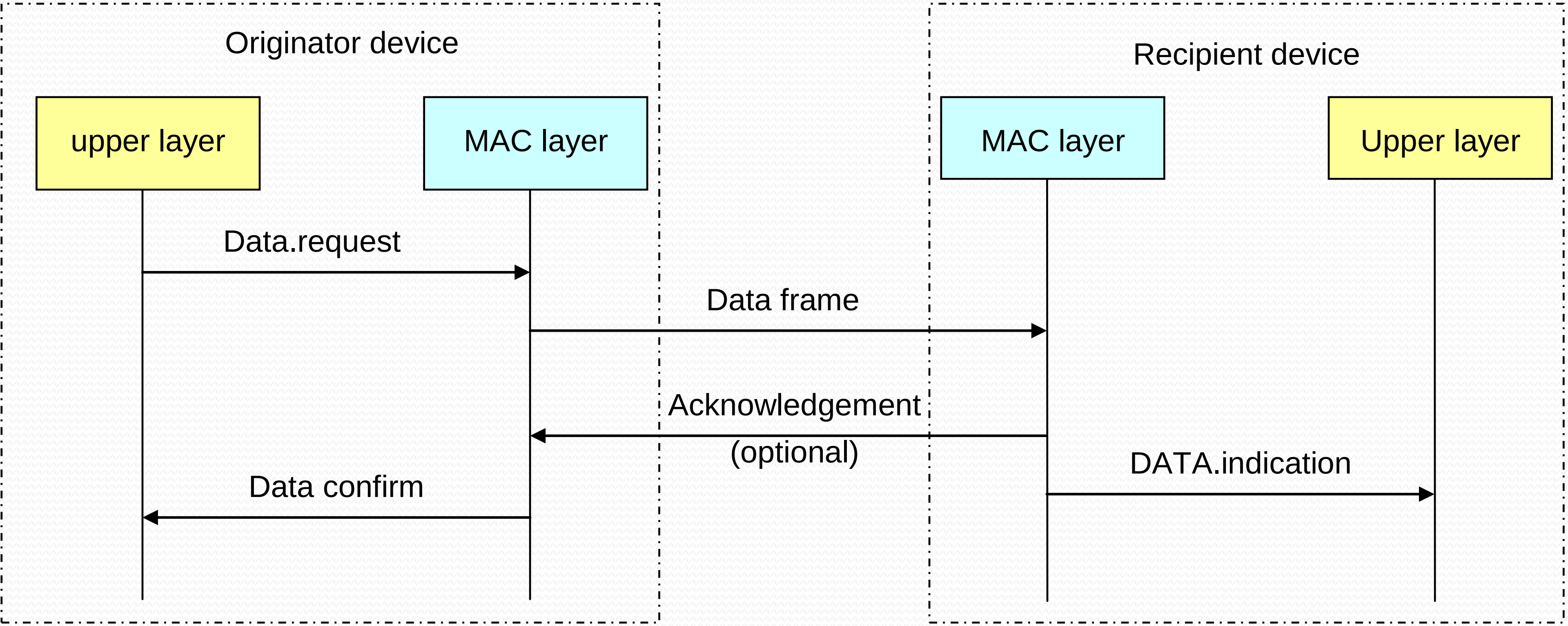


MAC layer data service

The data service

- Exploits only the request, confirm and indication primitives.
- 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.

MAC layer data service



MAC layer management services

The Management services

- Functionalities for:
  - PAN initialization
  - Devices association/disassociation
  - Detection of existing PANs
  - Other services to exploit the features of the MAC layer.

MAC layer management services

The Management services (O means optional for RFDs)

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 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.

MAC layer management services

The Associate service (on the end-device side)

- is invoked by a device wishing to associate with a PAN which it have already identified by preliminary invoking the SCAN service.
- 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.
  - Since 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.

MAC layer management services

The Associate service (on the coordinator side)

- The association request message is passed to the upper layers (with the ASSOCIATION.indication primitive)
  - The upper layer takes the actual decision about the association
- If the request is accepted the upper layer:
  - selects a short 16 bit address for the device
    - To be used in place of the 64-bit extended IEEE address.
  - invokes the ASSOCIATE.response primitive of the coordinator MAC layer.
    - 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

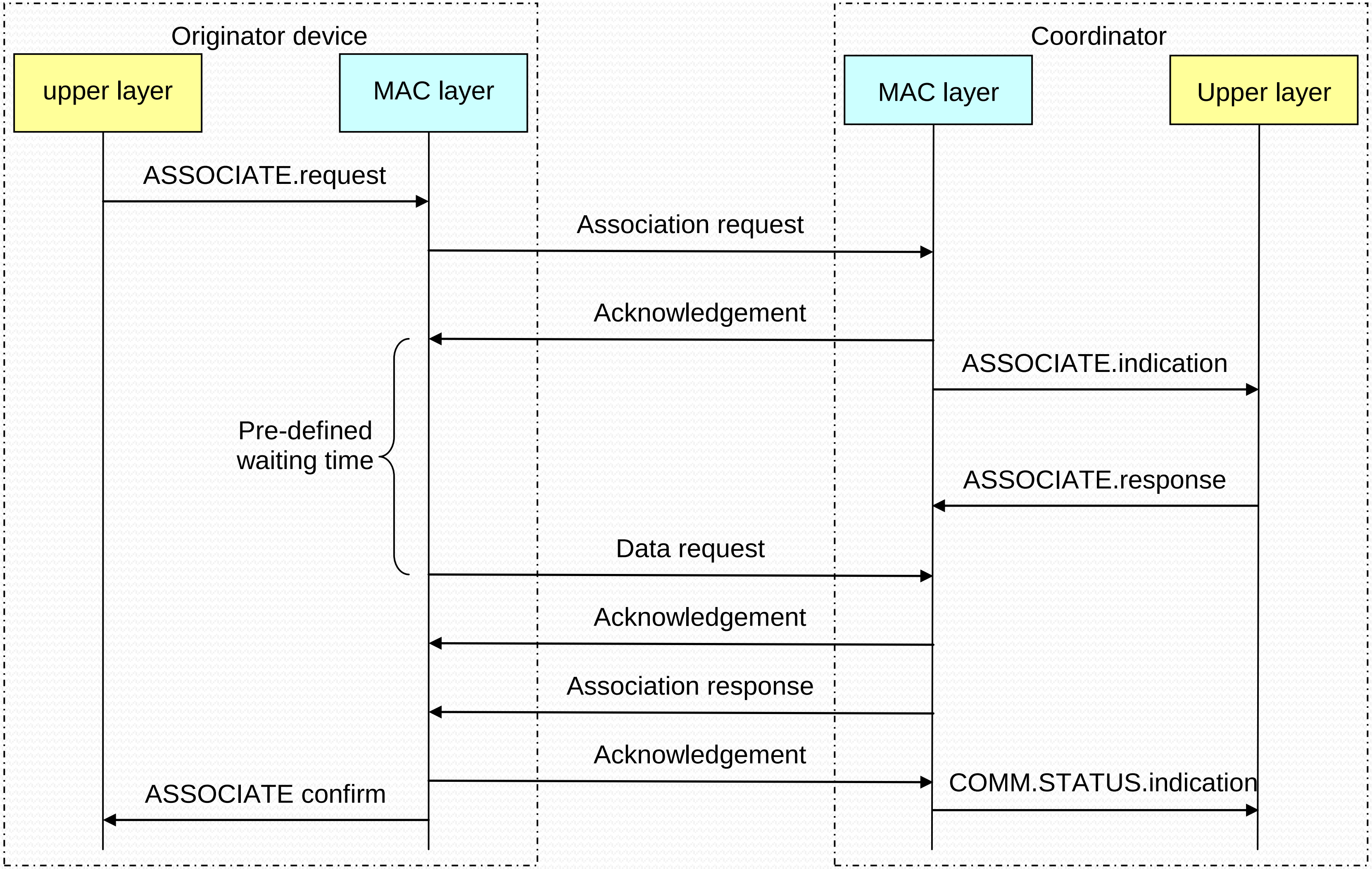
The end device MAC layer:

- issues a ASSOCIATE.confirm primitive to the upper layer

The coordinator MAC layer:

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

MAC layer management services



Implementation of the ASSOCIATE service

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.

MAC layer security

- **Access control**:
  - each device maintains a Access Control List (ACL) of devices with which it is enabled to communicate.
  - packets 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 or
  - The key can be shared between two peers

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.
  - The encryption/decryption key can be shared by a group of devices or
  - The key can be shared between two peers
  - Integrity may be provided on data, beacon and command frames.
- **Sequential freshness**:
  - orders the sequence of input frames to ensure that an input frame is more recent than the last received frame.

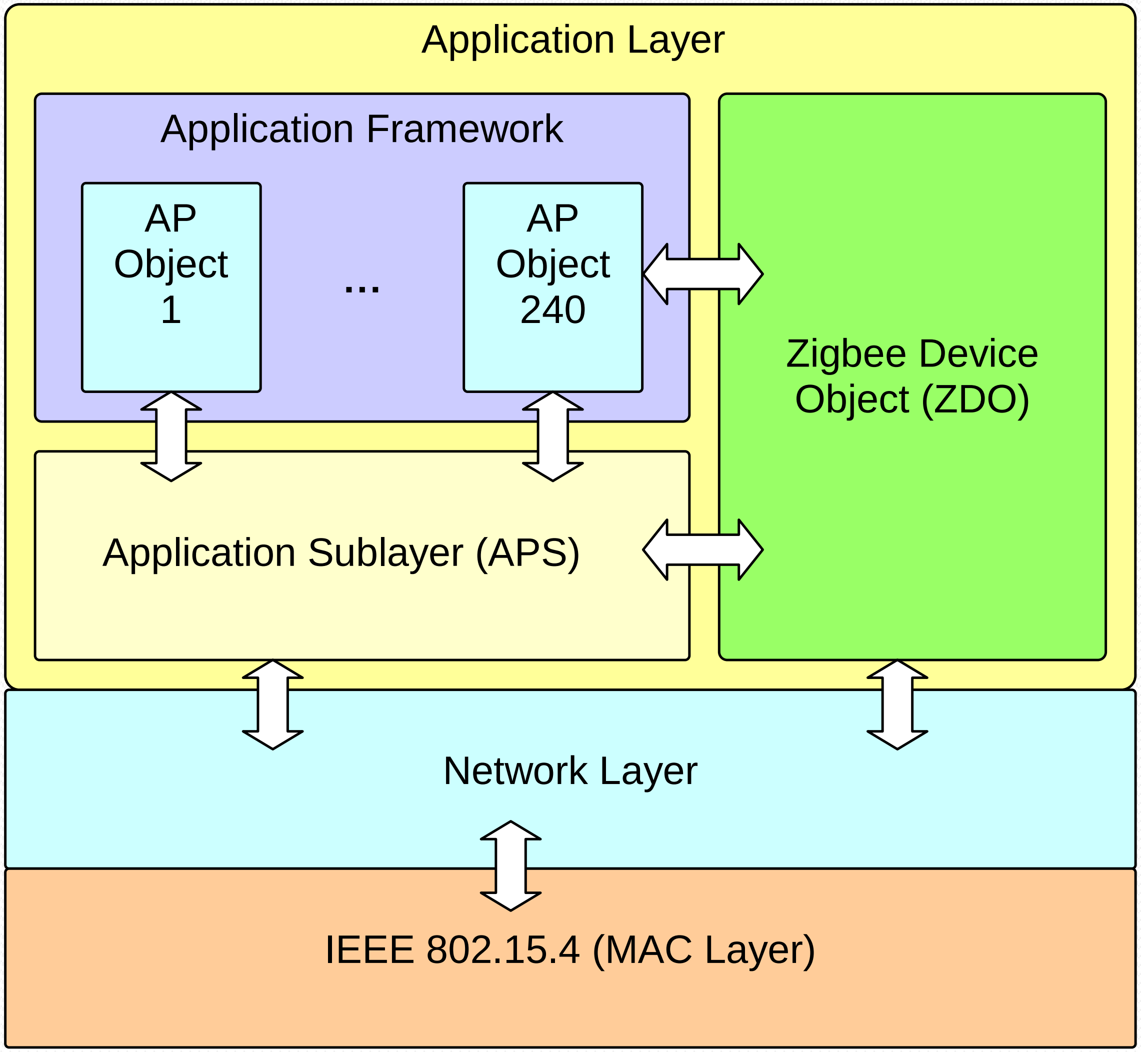
Part II

The ZigBee standard

The ZigBee standard

- Built upon the IEEE 802.15.4 standard.
- Specifies the network and the application layers
- The network layer:
  - Supports star, tree, and peer-to-peer multi-hop network topologies
- The application layer comprises:
  - The Application Framework
    - Contains up to 240 Application Objects (APO)
      - user defined application modules which implement a ZigBee application.
  - The ZigBee Device Objects (ZDO)
    - Provides services to let the APOs organize into a distributed application.
  - The Application Support sublayer (APS).
    - Provides data and management services to the APOs and ZDO.

The ZigBee standard

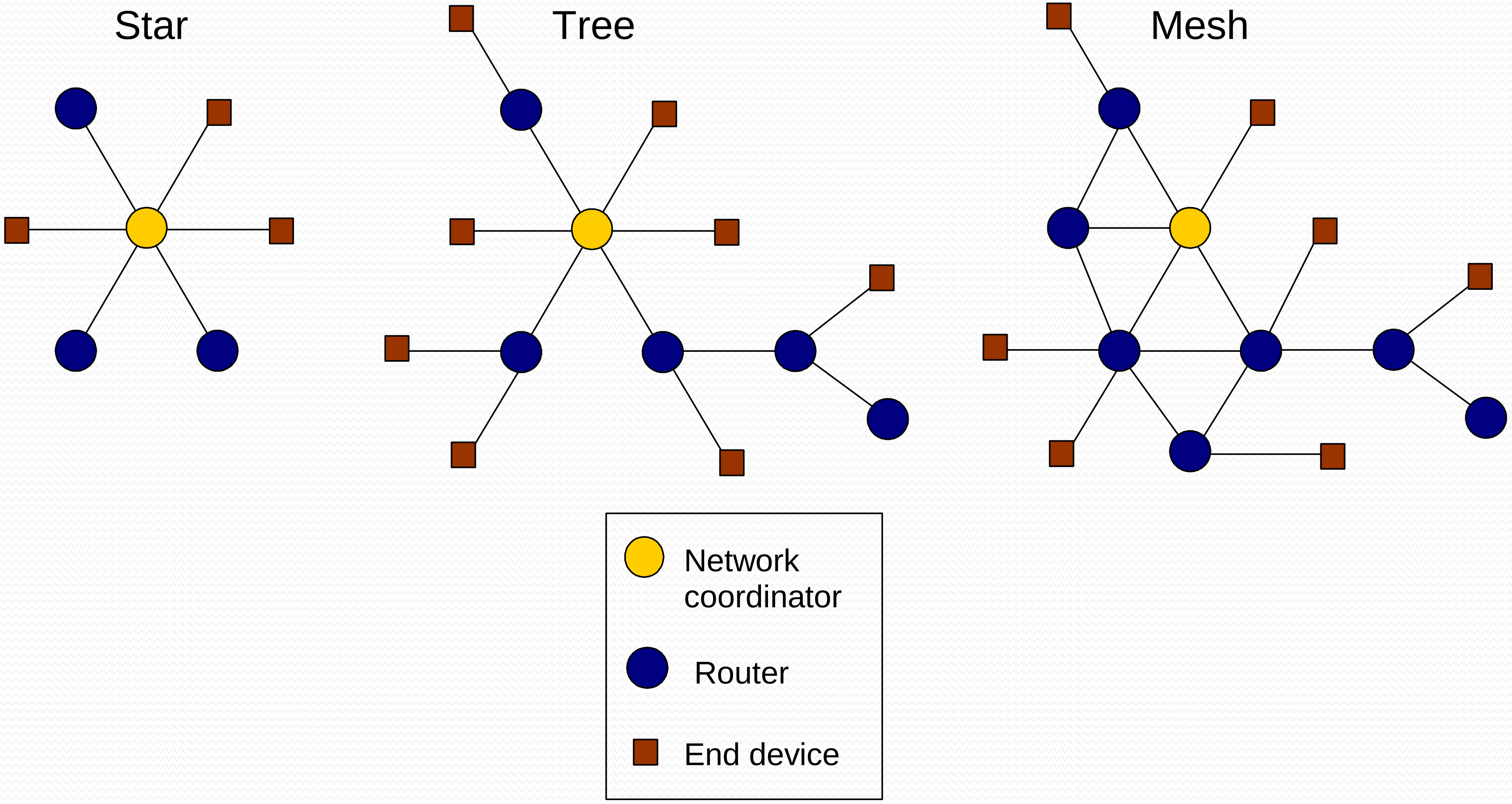


Network layer

Network layer

- Three types of devices
  - End-devices
    - Correspond to a RFD or to a FFD acting as a simple device,
  - Routers
    - A FFD with routing capabilities
  - The network coordinator
    - A FFD managing the whole network.
- Three topologies:
  - Star
    - Naturally maps to the star topology in IEEE 802.15.4
    - Uses the superframe structure
  - Tree
    - Can use the superframe structure
  - Mesh
    - Communications without the superframe structure

Network layer: topologies



Network layer

- Services for:
  - Network initialization
  - Devices addressing
  - Routes management & routing
  - Management of connections/disconnections of devices.

Network layer: services

Name	Request	Indication	Confirm	Description
DATA	X	X	X	Data transmission service
NETWORK-DISCOVERY	X		X	Look for existing PANs
NETWORK-FORMATION	X		X	Create a new PAN (invoked by a router or by a coordinator)
PERMIT-JOINING	X	X	X	Allows associations of new devices to the PAN (invoked by a router or by a coordinator)
START-ROUTER	X		X	(Re-)initializes the superframe of the PAN coordinator or of a router
JOIN	X	X	X	Request to join an existing PAN (invoked by any device
DIRECT-JOIN	X		X	Request to other devices to join the PAN (used by routers or by the coordinator)
LEAVE	X	X	X	Leave a PAN
RESET	X		X	Resets the network layer
SYNC	X		X	Allows the application layer to synchronize with the coordinator or a router and/or to extract pending data from it
GET	X		X	Reads the parameters of the network layer
SET	X		X	Set parameters of the network layer

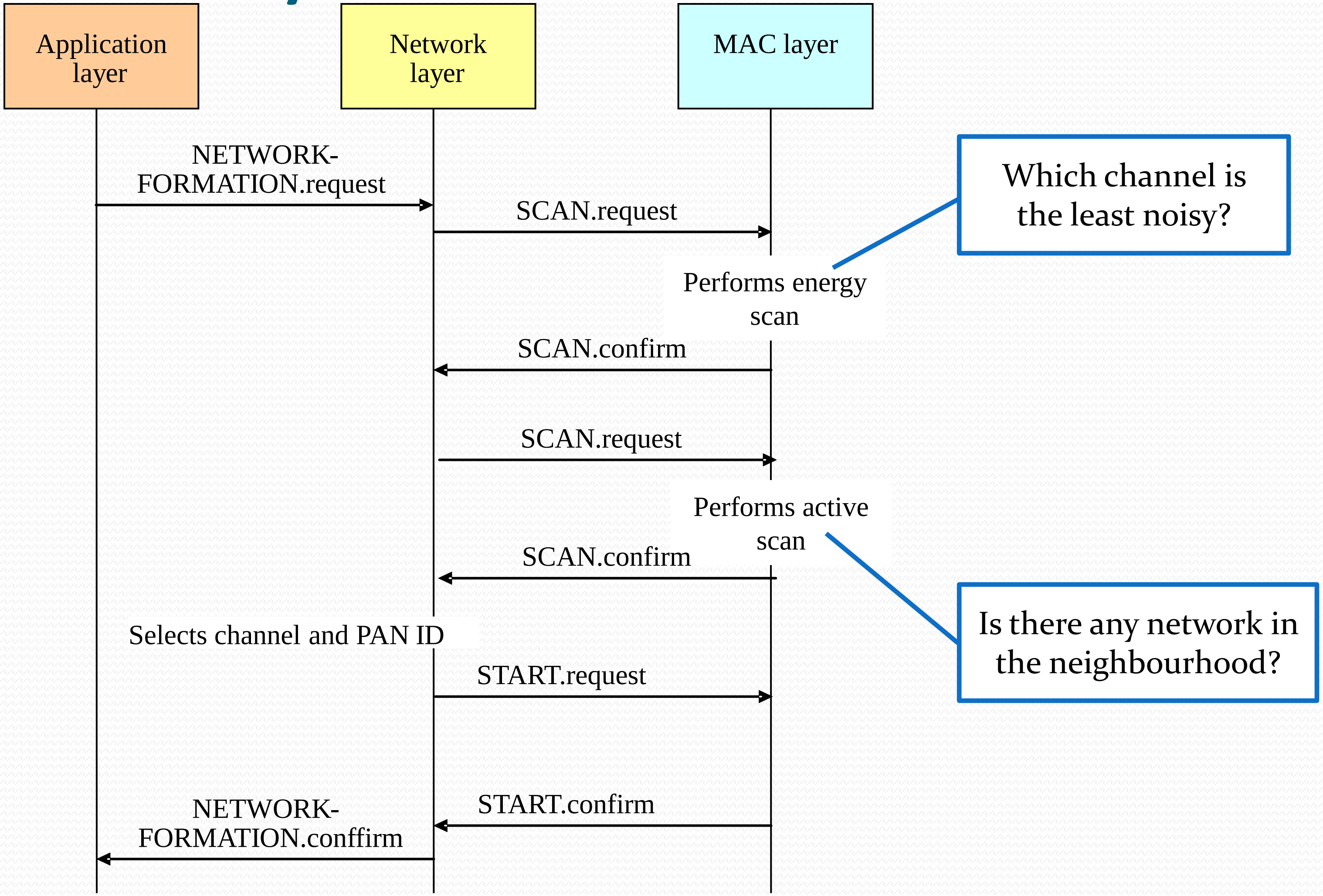
Network layer

- Before any ZigBee device may communicate on a network, it must either:
  - Form a new network → ZigBee Coordinator
  - Join an existing network → ZigBee router or end-device
- The role of the device is chosen at compile-time

Network layer: network formation

- Initiated by the NETWORK-FORMATION.request primitive.
  - This primitive can be invoked only by devices that can behave as coordinator and that are not currently joined to another network.
  - Uses the MAC layer services to look for a channel which does not conflict with other existing networks.
  - Selects a PAN identifier which is not already in use by other PANs,
  - Assigns itself (the PAN coordinator) the 16-bit network address 0x0000.
  - Invokes the SET.request primitive of the MAC layer to set the PAN identifier and the device address;
  - Invokes the START.request primitive of the MAC layer to start the PAN.
    - In response to this primitive the MAC layer begins generating the beacons

Network layer: network formation



Network layer: joining a network

- Join through association: initiated by a device wishing to join an existing network

- Direct join: requested by a router or by the coordinator to request a device to join its PAN (direct join).

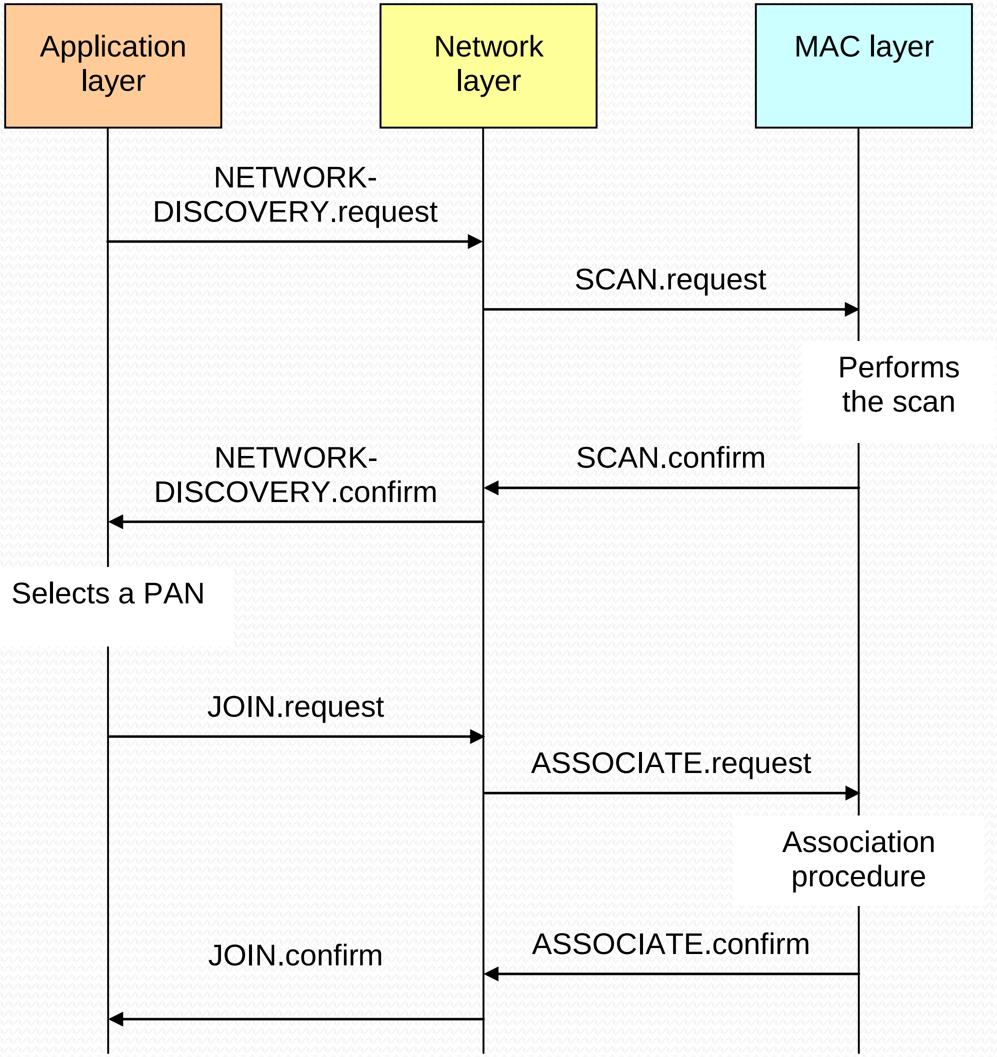
Network layer: joining a network

Join through association: the device wishing to join a network:

- Performs a NETWORK-DISCOVERY to look for existing PANs.
- Invokes JOIN.request with parameters:
  - The PAN identifier of the selected network
  - A flag indicating whether it joins as a router or as an end device.
- The JOIN.request primitive in the network layer selects a "parent" node *P* (in the desired network) from his neighbourhood.
  - In the case of the star topology, the parent is the coordinator and the devices join as an end device.
  - In the tree the parent must be a router or the coordinator and the device joins as a router or as an end device
- Receives from the parent a 16-bit short address
  - To be used in any further network communication.

Network layer: joining a network

Join procedure at the child’s side.



Network layer

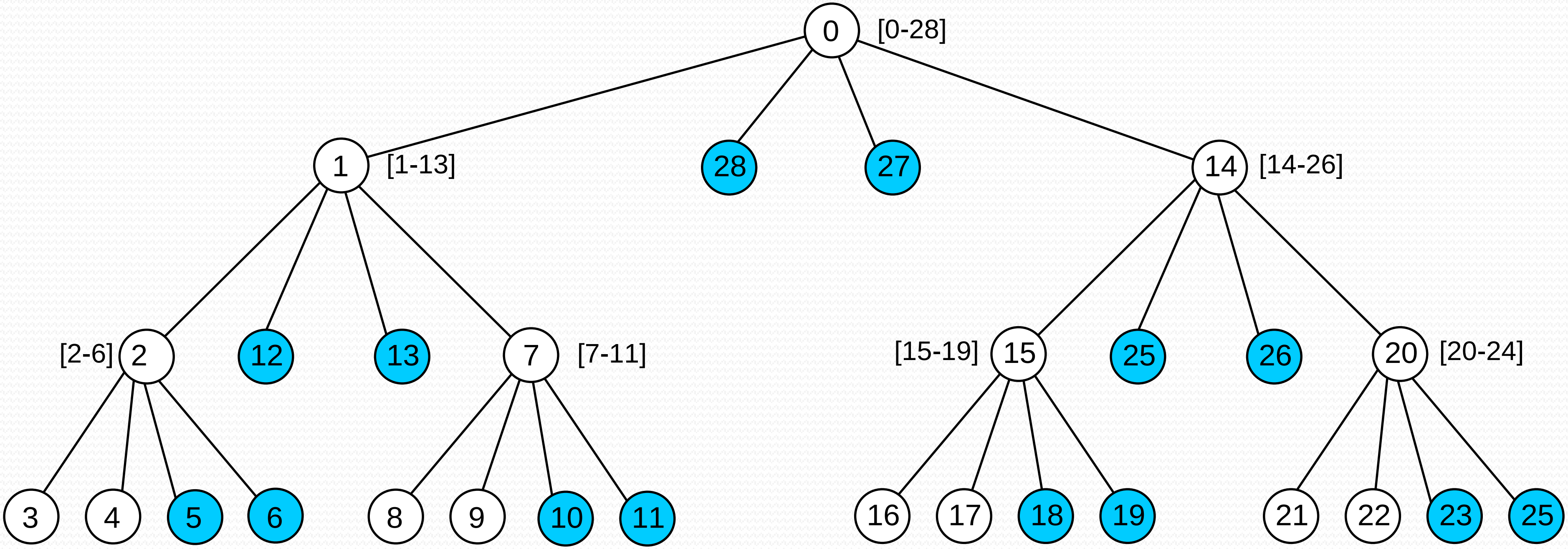
- The parent-child relationships established as a result of joins, shape the whole network in the form of a tree:
  - The ZigBee coordinator is the root
  - The ZigBee routers are internal nodes
  - The ZigBee end-devices are the leaves.

Network layer

- This tree is used to assign the short addresses
- The ZigBee coordinator fixes:
  - The maximum number of routers (*Rm*) each router may have as children
  - The maximum number of end-devices (*Dm*) that each router may have as children
  - The maximum depth of the tree (*Lm*).
- Each router is assigned a range of addresses
  - To assign addresses to its children
  - Computed based on *Rm*, *Dm*, and *Lm*.
- Devices join as high up the tree as possible → it minimizes the number of hops
- Although the addresses are assigned according to a tree structure the actual topology can be a mesh.

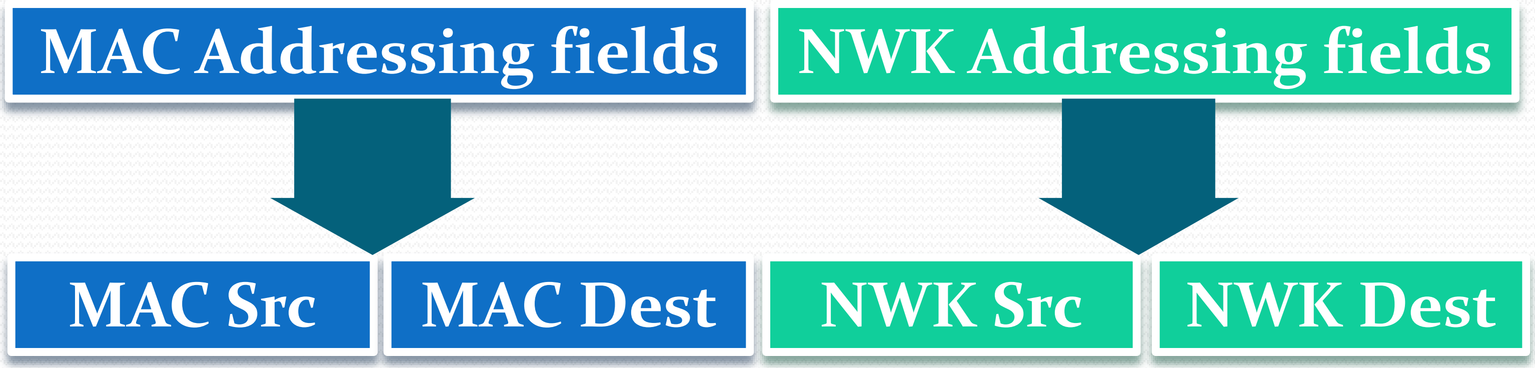
Network layer

- Address assignment in a network with *Rm*=2, *Dm*=2 and *Lm*=3
  - Routers (white nodes)
  - End-devices (blue nodes).



Exercise

- Question: Why have two addresses fields in both MAC header and NWK header?



MAC Addressing fields

NWK Addressing fields

MAC Src

MAC Dest

NWK Src

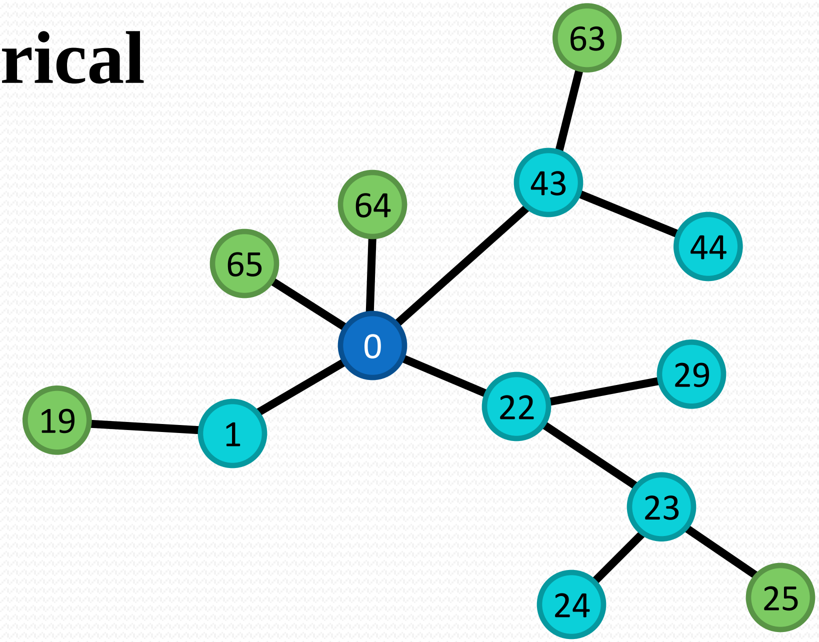
NWK Dest

Answer

- If sending a packet from node A to node K, the firest hop would be from A to B, the second hop from B to C, and so on until the final hop from J to K.
- The addresses NWK Src and NWK Dest always indicate resp. A and K, while the MAC Src and MAC Dest are per-hop addresses, A to B, and so on. This is a difference of address range.

Exercise

A symmetrical tree



Lm	3
Dm	5
Rm	3

- For each depth level, compute the max number of nodes.

Answer

- Consider node 24, it is at depth 3, then it cannot have children
- Consider node 23, it at depth 2 and may have up to 5 children (@24 to @28), then it can consume up to 6 addresses
- Node 22 is at depth 1. Then, it can have 1(itself)+3x6(3 routers max)+2(Dm-Rm)= 21 addresses.
- The coordinator is at depth 0. Then, it can have 1(itself)+3x21(3 routers max)+2(Dm-Rm)= 66 addresses

Network layer: routing

- A variety of methods:
  - Broadcasting
  - Mesh routing (node to node)
  - Tree routing (node to node)

Network layer: routing

Routing

- Based on AODV
- If the sender is an end device it forwards the message to its parent.
- If the sender is a router or the coordinator it maintains a Routing Table and it routes the message according to the routing procedure.

Field Name	**Size**	**Description**
Destination Address	16 bits	network address of the destination
Next-hop Address	16 bits	network address of next hop towards destination
Entry Status	3 bits	Route status: Active, Discovery_underway, Discovery_failed, or Inactive

Table 5: Routing Table (RT) in a ZigBee router.

Network layer: routing

Routing protocol in a mesh

- If the routing table does not contains an entry for the destination
    - Performs a route discovery
- Otherwise the packet is forwarded according to the routing table

Routing protocol in a tree

- Packets routed along the tree based on the destination address

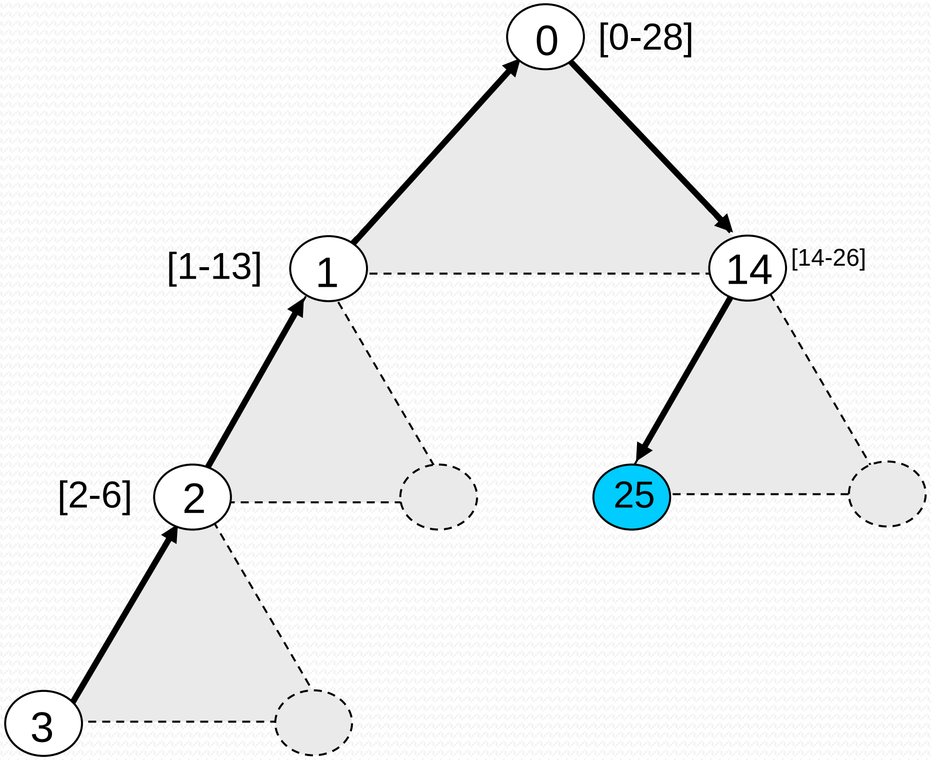
The tree and mesh topologies may live together:

- The routers can maintain both information for mesh and tree routing.
- The routing algorithm may switch between the two modes.

Considerations:

- Mesh routing does not allow beaconing
- Tree routing may allow beaconing
    - the relay routers must synchronize with their parents or childs beacon frame)

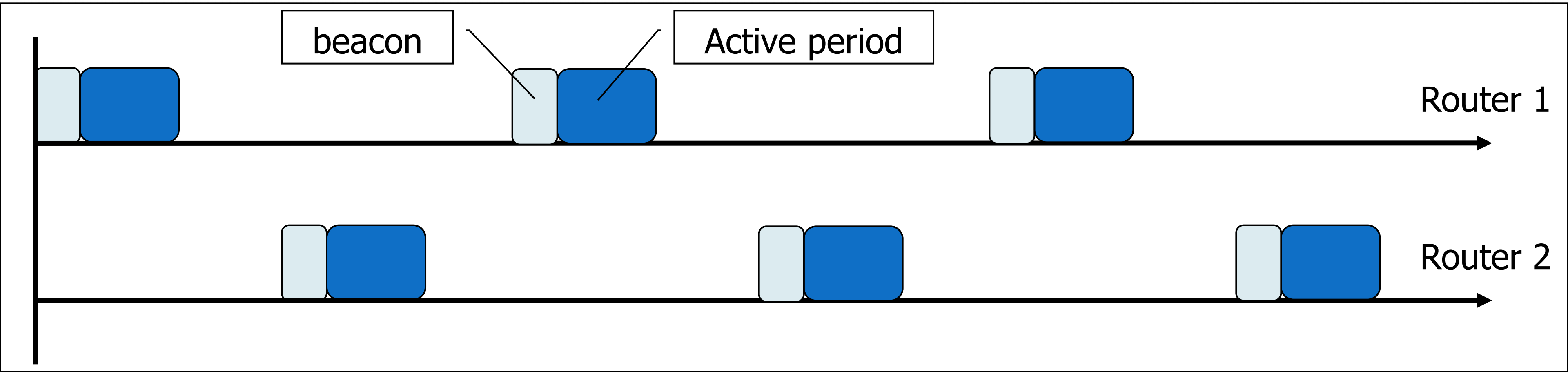
Network layer: tree routing



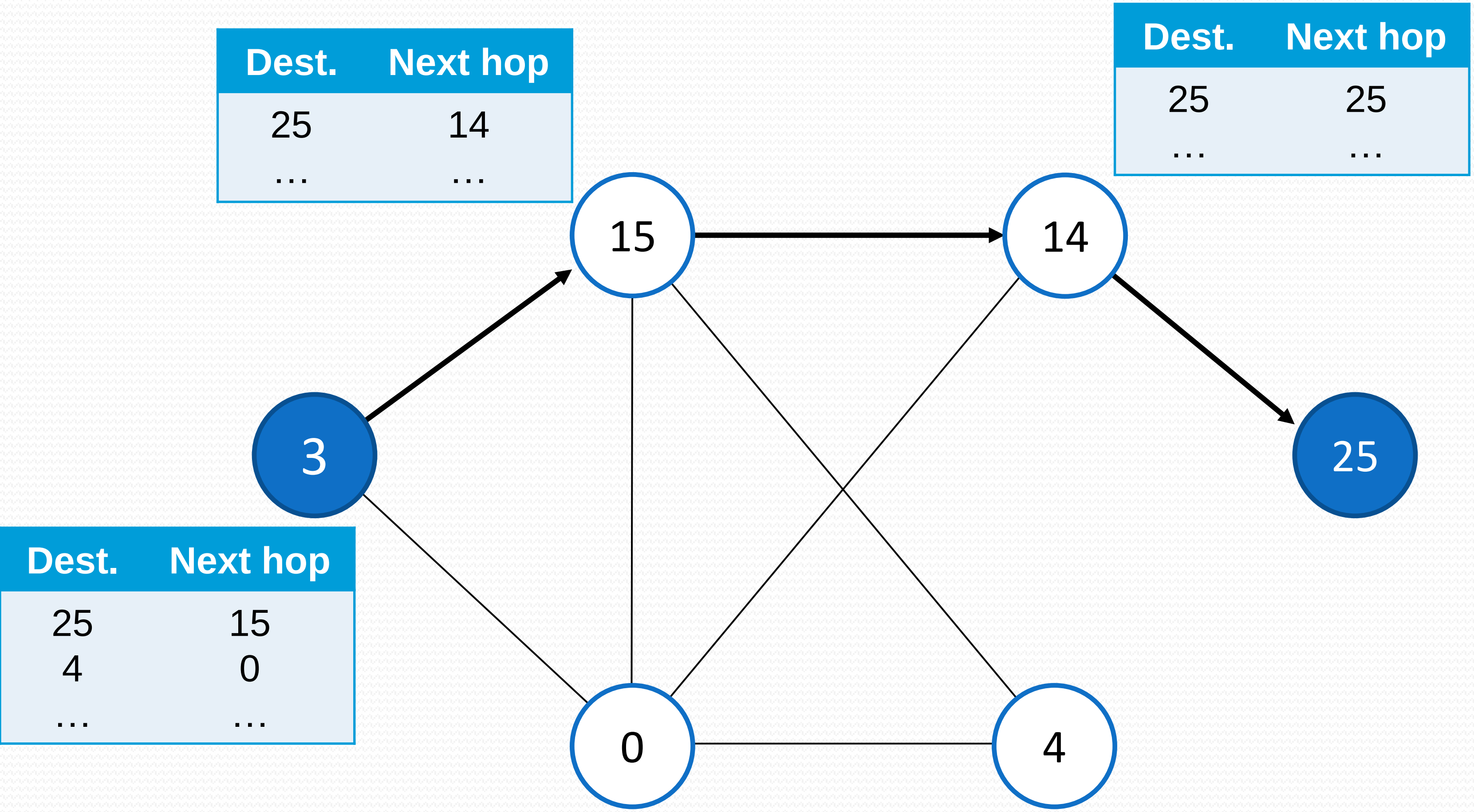
Network layer: tree routing

Beaconing in the tree topology

- Beacon scheduling is necessary to prevent the beacons of one router from colliding with either the beacons or data transmissions of its neighbouring devices
- The idea is to have short active portions as compared to the beacon interval
  - Avoids overlapping beacons of neighbouring routers.
  - The larger is the inactive period, the more devices that can transmit beacon frames in the same neighborhood



Network layer: mesh routing



Dest.	Next hop
25	14
…	…

Dest.	Next hop
25	25
…	…

Dest.	Next hop
25	15
4	0
…	…

Network layer: mesh routing

- Route discovery protocol:
  - Initiated if the routing table does not contain a valid entry for the destination
  - Routers maintain a Route Discovery Table (RDT)

Field Name	Size	Description
RREQ ID	8 bits	Unique ID (sequence number) given to every RREQ message being broadcasted
Source Address	16 bits	Network address of the initiator of the route request
Sender Address	16 bits	Network address of the device that sent the most recent lowest cost RREQ
Forward Cost	8 bits	The accumulated path cost from the RREQ originator to the current device
Residual Cost	8 bits	The accumulated path cost from the current device to the RREQ destination
Expiration time	16 bits	A timer indicating the number of milliseconds until this entry expires.

Network layer: mesh routing

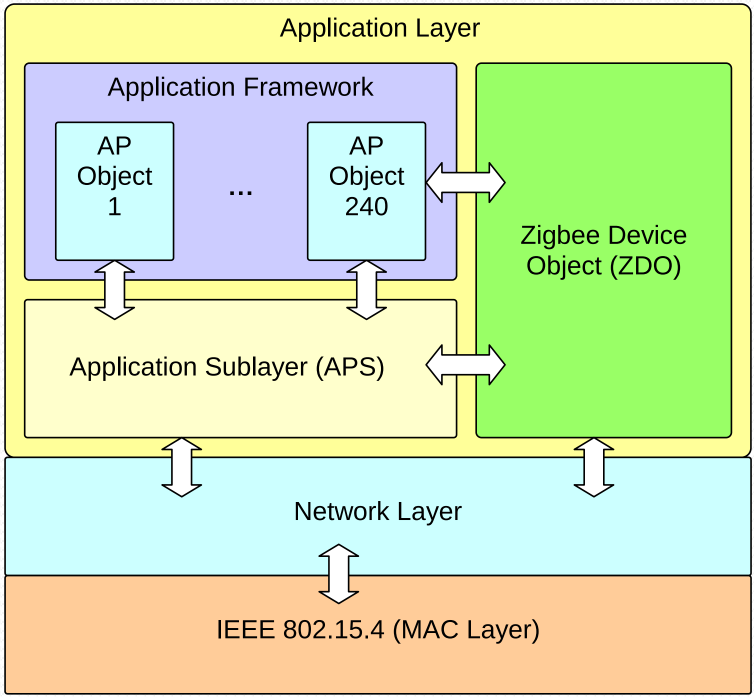
Route discovery protocol

- Broadcasts a route discovery message (RREQ)
  - Contains the RREQ ID, the destination address and the path cost which is initially be set to 0.
  - As the RREQ propagates in the network intermediate devices update their table and forward the RREQ
  - Each intermediate device also update the path cost using link cost estimations provided by the IEEE 802.15.4 interface.
  - An intermediate node may reply to the RREQ
  - The destination replies with a route reply
- The route reply:
  - Travels in unicast to the route discovery originator

Application layer

Application Layer

- The Application layer comprises:
  - The Application Framework
    - includes a set of Application Objects (APO).
  - The Zigbee Device Object (ZDO)
    - Manages the application services
  - Application Support Sublayer (APS)
    - Provides data, binding, and discovery services.

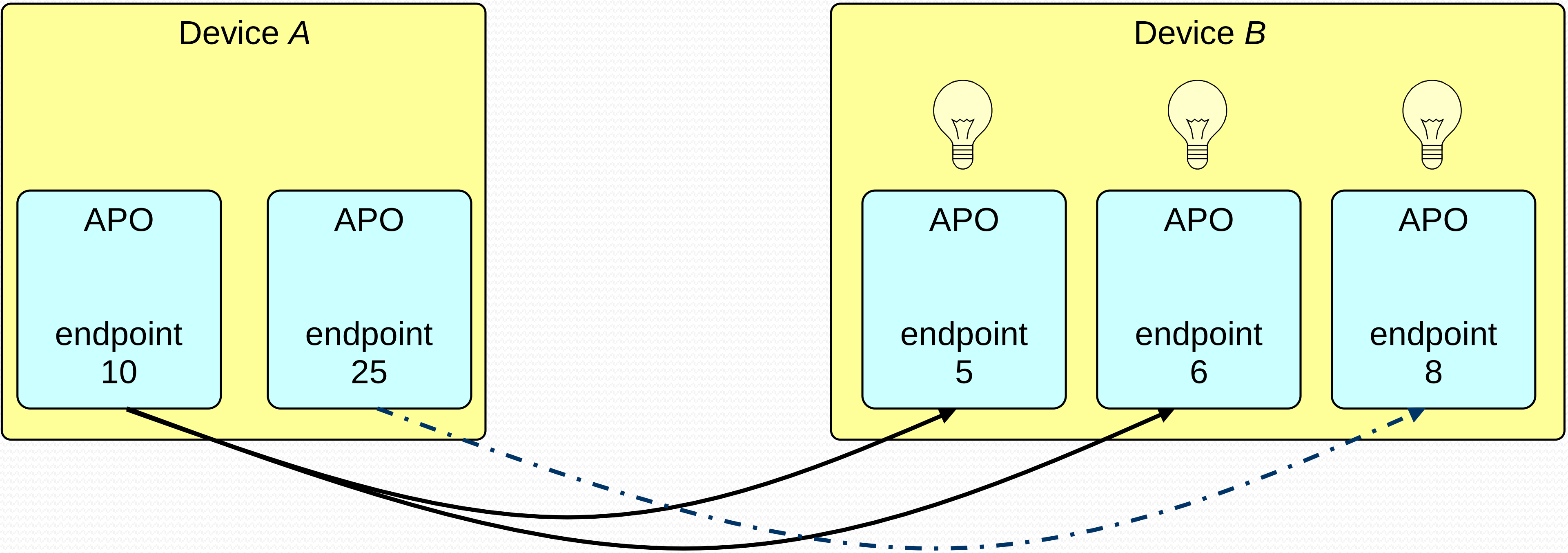


The application framework

- Up to 240 APOs, each corresponding to an application endpoint
- Endpoint 0 is reserved for the ZDO.
- Each APO in the network is uniquely identified by its endpoint address & the network address of the hosting device.
- Simplest APO can be queried with Key Value Pair data service (KVP)
    - Set/Get/Event transactions on the APOs attributes
    - KVP disappeared in the most recent versions of ZigBee
- More complex APOs can have complex states and communicate the Message data service.

A simple application

- the APOs 5*B*, 6*B*, and 8*B* have a single attribute containing the status of the lamp (on/off) which can set remotely from the APOs 10*A* and 25*A*



Application Support Sublayer

- The APS frame includes endpoints, clusters and profile IDs.
- APS is responsible for:
  - Data service (a light transport layer)
    - Filtering out packets (non registered endpoints, profiles that don’t match)
    - Generating end-to-end acknowledgment
  - Maintaining:
    - the local binding table
    - The local groups table
    - The local address map

Addressing in APS

- Addressing requires the following components:
  - EndPoint
  - Cluster
  - Profile ID
- ZigBee defines clusters and profiles to standardize the applications

Endpoints

- In each node Endpoints are identified by a number between 1 and 240.
- A ZigBee node can run multiple applications.
- Endpoints are seen as virtual wires connecting applications
- They allow for separate profiles, devices and control points to co-exist within a single node

Clusters

- Defined by a 16 bit identifier
- Application meaning
- Example : ID 0x0006 is a cluster that knows how to turn something on/off
- Clusters have meaning within a particular profile
- They contain both commands and attributes
  - Commands cause action on a device
  - Attributes show the state of a given cluster

ZigBee Clusters

Cluster Name	Cluster ID
Basic Cluster	0x0000
Power Configuration Cluster	0x0001
Temperature Configuration Cluster	0x0002
Identify Cluster	0x0003
Group Cluster	0x0004
Scenes Cluster	0x0005
OnOff Cluster	0x0006
OnOff Configuration Cluster	0x0007
Level Control Cluster	0x0008
Time Cluster	0x000a
Location Cluster	0x000b

Application Profile

- An application profile is the specification in a standard format of the behaviour of an application possibly operating on several ZigBee devices.
  - An application profile describes a set of devices and clusters.
  - The application profiles are assigned with a unique identification number which is assigned by the ZigBee alliance.

Profiles

- Every data is sent (received) on an application profile
- Profile ID are 16 bit numbers
  - Public profiles range from 0x0000 to 0x7fff
  - manufacturer profiles range from 0xbf00 to 0xffff
- Profiles can be seen as domain spaces of related applications and devices.
- Any number of Application profiles may exist in a single ZigBee network.

Profile IDs

Profile ID	Profile name
0101	Industrial Plant Monitoring
0104	Home Automation
0105	Commercial Building Automation
0107	Telecom Applications
0108	Personal Home & Hospital Care
0109	Advanced Metering Initiative

Device IDs

- ZigBee device IDs range from 0x0000 to 0xFFFF.
- They have two purposes:
  - To allow human-readable displays (e.g., an iconis related to a device)
  - To allow ZigBee tools to be more effective.
- ZigBee performs service discovery based on profile IDs and cluster IDs, but not on device IDs

Device IDs

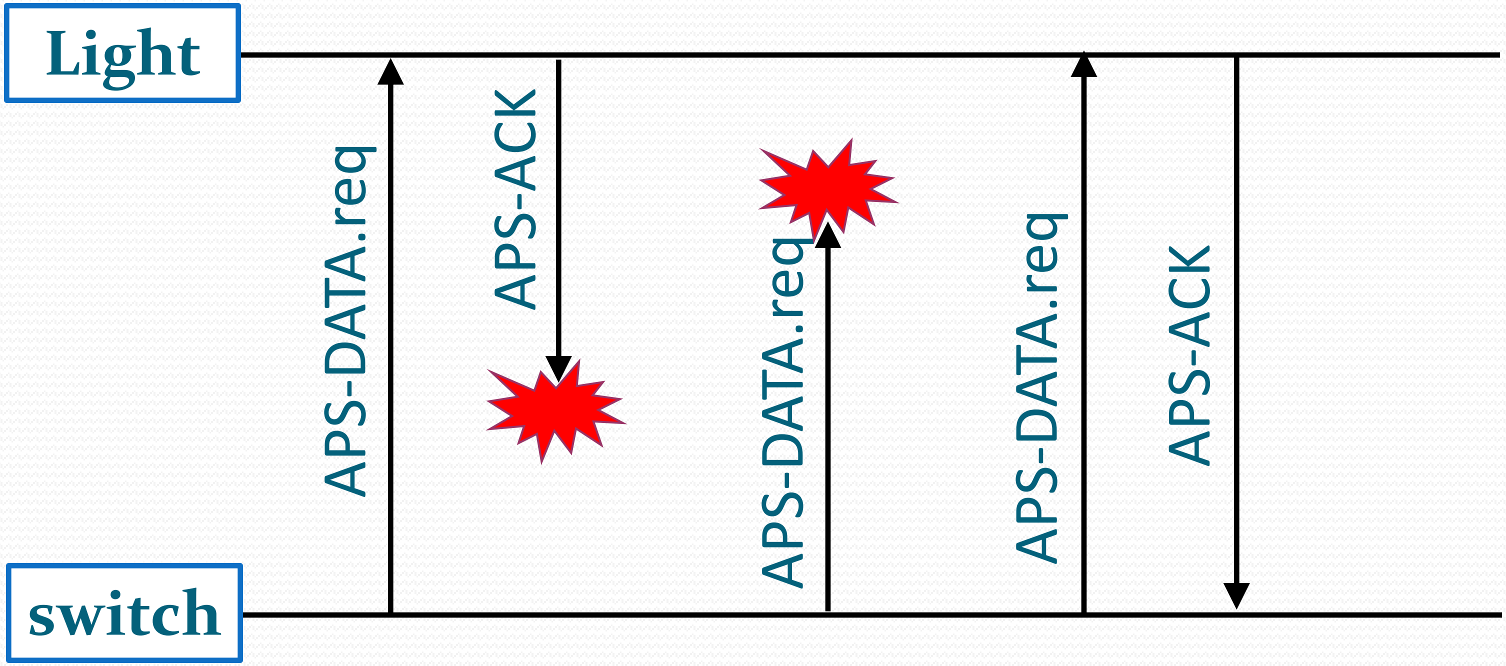
- Example in the Home Automation Profile

Name	Identifier	Name	Identifier
Range Extender	0x0008	Light Sensor	0x0106
Main Power Outlet	0x0009	Shade	0x0200
On/Off Light	0x0100	Shade Controller	0x0201
Dimmable Light	0x0101	Heating/Cooling Unit	0x0300
On/Off Light Switch	0x0103	Thermostat	0x0301
Dimmer Switch	0x0104	Temperature Sensor	0x0302

APS Services

- Offers the binding service to the ZDO and a data service to both the APOs and the ZDO.
- APS data service: enables the exchange of messages between two or more devices within the network using either direct or indirect addressing.
  - The data service is defined in terms of the primitives:
    - request (send),
    - confirm (returns status of transmission) and
    - indication (receive).

Example: ACK


Light
switch
APS-DATA.req
APS-ACK
APS-DATA.req
APS-DATA.req
APS-ACK

APS Binding

- Allows an endpoint on a node to be connected (bound) to one or more endpoints on other nodes.
- Binding is unidirectional
- Comprises the BIND and UNBIND
- Can be used only by the ZDO of the coordinator or of a router.
  - BIND.request creates a new entry in the local binding table
    - Takes in input the tuple <source address, source endpoint, cluster cluster identifier, destination address, destination endpoint>
  - UNBIND.request deletes an entry from the local binding table.

APS Binding

- The binding provides a way to address the destination of messages (Indirect addressing)
  - A message is normally routed to the destination APO based on its address pair <destination endpoint, destination network address> (direct addressing)
  - Direct addressing might be unsuitable for extremely simple devices
  - Indirect addressing exploit binding tables
    - The table matches source address (in terms of network and endpoint address) and the cluster identifier into the pair <destination endpoint, destination network address>.
    - The binding table is stored in the ZigBee coordinator and/or in the routers and it is updated on explicit request of the ZDO in the routers or in the coordinator.

Binding Table

Src EP	Dest Addr	Addr/Grp	Dest EP	Cluster ID
5	0x1234	A	12	0x0006
6	0x796F	A	240	0x0006
5	0x9999	G	_	0x0006
5	0x5678	A	44	0x0006

- Example: a APS-DATA.req from EP 5 (indirect) will generates 3 data requests, one to node 0x1234 endpoint 12, one broadcast to group 0x9999 and the last to node 0x5678 endpoint 44.

APS Address Map

- The APS layer contains the address map table.
- Associates the 16 bit NWK address with the 64 bit IEEE MAC address.
- Mobile devices (ZED) may change their 16 bit NWK address. In that case an announcement is sent on the network and every node updates its internal tables to preserve the binding.

APS Address Map

NWK Addr	IEEE Addr
0x0000	0x0030D237B0230102
0x0001	0x0030B237B0235CA3
0x895B	0x0031C237b023A291

- Example of APS address map

ZigBee Device Object

- ZDO is a special application attached to endpoint 0
- Implements ZigBee End Devices, ZigBee Routers and ZigBee Coordinators.
- It is specified by a special profile, the ZigBee Device Profile, which describes the clusters that must be supported by any ZigBee device.
  - In particular the ZigBee Device Profile defines how the ZDO should implement the services of discovery and binding and how it should manage the network and the security.

ZigBee Device Object

ZDO services:

- **Device and service discovery**
- **Binding management**
- **Network management**
- **Node management**

Device and service discovery

- The ZigBee Device Profile (ZDP) contains a set of commands for discovering various aspects about nodes.
- Device discovery
  - the coordinator returns the address of its associated devices
  - Allows a device to obtain the (network or MAC) address of other devices in the network.
  - A router or the coordinator responds to a device discovery query by returning its address and the address of all the end devices associated to them

Device and service discovery

- Service discovery
  - The coordinator responds to queries based on cluster IDs, addresses, or device descriptors and returns lists of endpoint addresses matching with the query

Binding

- The ZDO processes the binding requests received from local or remote EP adding or deleting entries from the APS binding table.
- Requires an IEEE address.

Src EP	Dest addr	Addr/grp	Dest EP	Cluster ID
7	0x4321	A	23	0x0006
10	0x44AB	A	130	0x0006
7	0x98FF	A	66	0x0006

Example of binding table

Managing network and nodes

- **Network management**
  - Implements the protocols of the coordinator, a router or an end device according to configuration settings established either via a programmed application or during installation.
- **Node management**
  - The ZDO serves incoming requests aimed at performing network discovery, retrieving the routing and binding tables of the device and manage joins/disconnections of nodes to the network.

Security

- Aimed at ensuring protection of individual devices **but not individual applications** in the same device.
  - This allows the re-use of the same keying material among the different layers on the same device
- Security requirements:
  - Message integrity (either at entire network or at device level)
  - Device authentication (either at entire network or at device level)
  - Message encryption
  - Message freshness (to avoid message duplicates).
- Keys:
  - Single key per network (network level security)
  - Single key per link (device level security)

Security

- Security at the network layer:
  - Securely transmit outgoing frames and securely receive incoming frames (AES-128 bit standard).
  - symmetric encryption and decryption using keys provided by the application layer.
  - In any case some command messages (such as association messages) cannot be encrypted.
- Security at the application layer:
  - Management of the keys and of the security policies.
  - Defines the **Trust Center,** an application-layer module (allocated in the coordinator or a router) and which provides the keys to the devices in the network.
  - The devices in the network establish a secure communication link with the trust center using the master key and use the secure link to request to the trust center the keys for their needs.
    - The master key could be either pre-assigned or provided to the devices using special procedures (it could be manually inserted by the user),