An Introduction to IEEE 802.15.4 (ZigBee)

Gao Chao
Vaasa Polytechnic
Vaasa, Finland

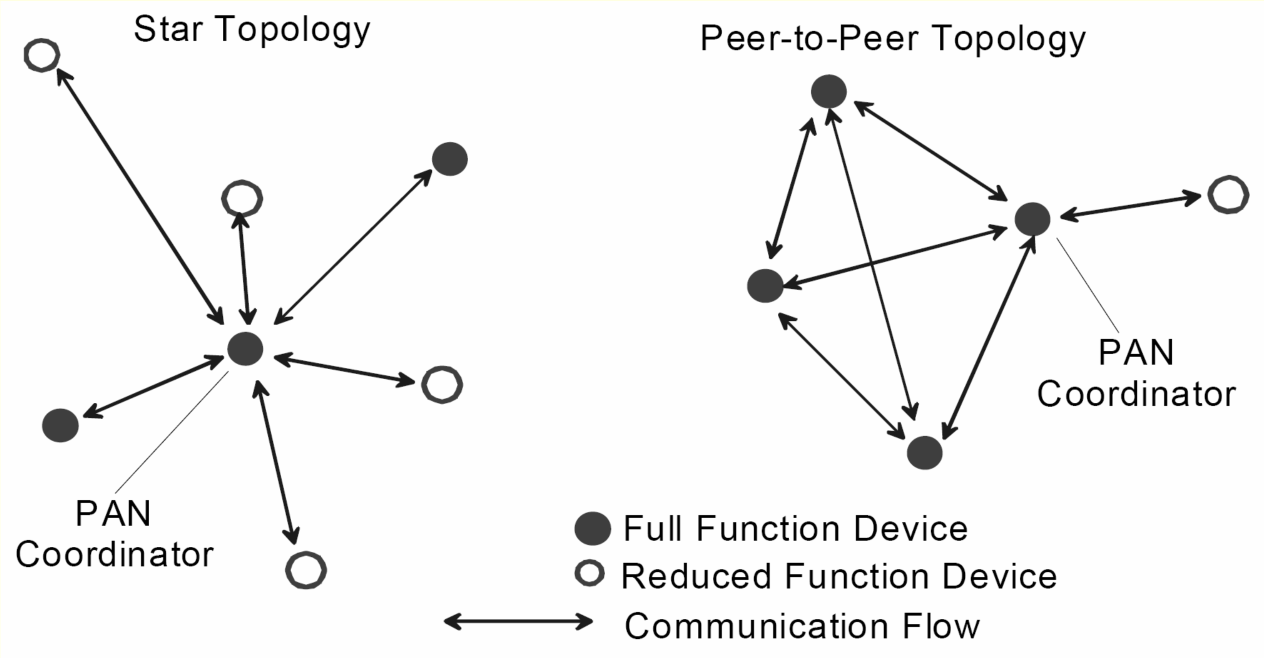
General Description

- Over-the-air data rates of 250 kb/s, 40 kb/s, and 20 kb/s
- Star or peer-to-peer operation
- Allocated 16 bit short or 64 bit extended addresses
- **Allocation of guaranteed time slots (GTSs)**
- Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) channel access
- Fully acknowledged protocol for transfer reliability
- Low power consumption
- Energy detection (ED)
- Link quality indication (LQI)
- 16 channels in the 2450 MHz band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band

Aimed to a Low-Rate Wireless Personal Area Network (LR-WPAN) Standard.

Network Topologies

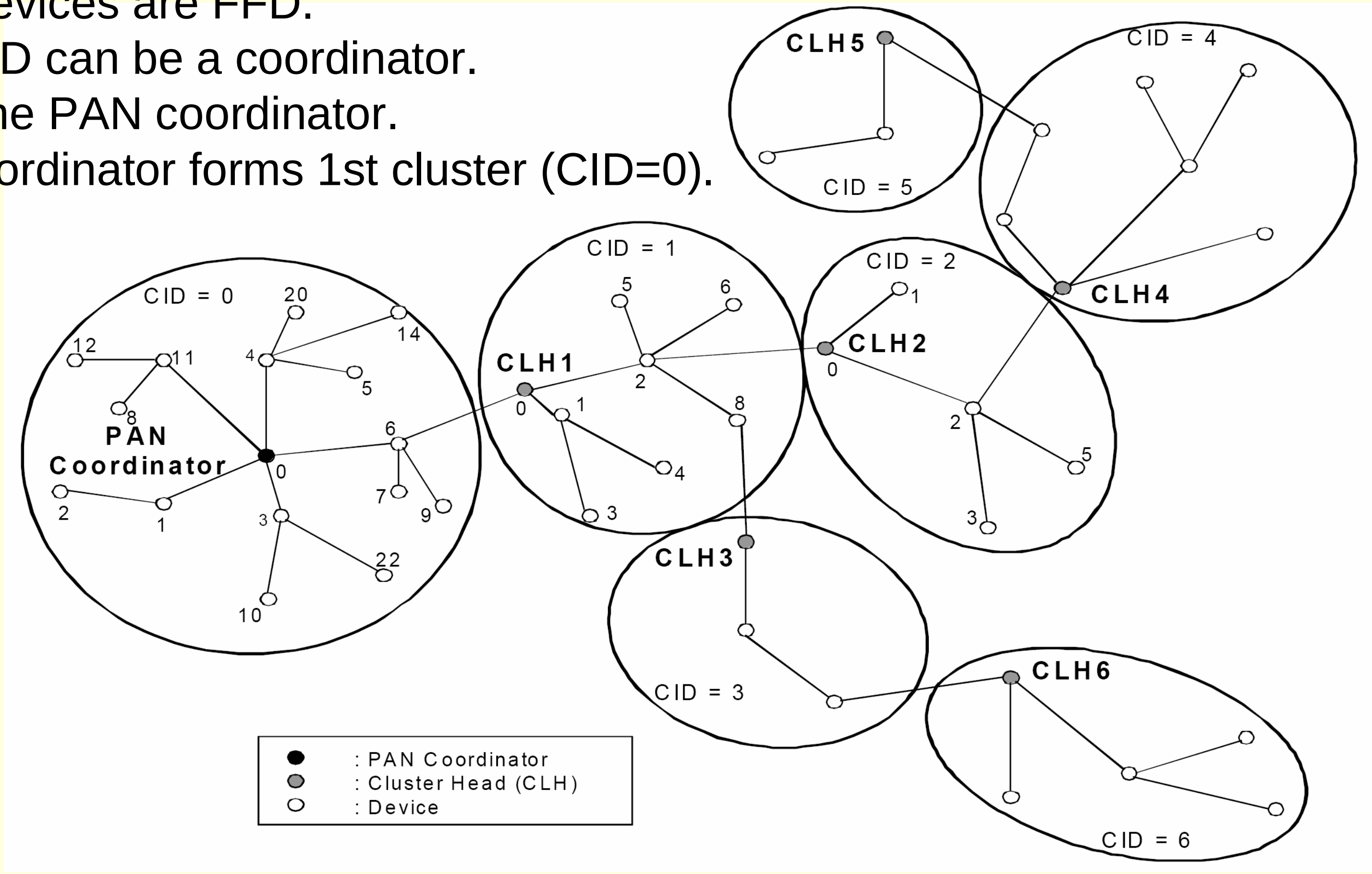
- Star: a FFD (Full-Function Device) works as coordinator, other FFD and RFD (Reduced Function Device) in range as slaves.
- Peer-to-Peer: ad hoc network



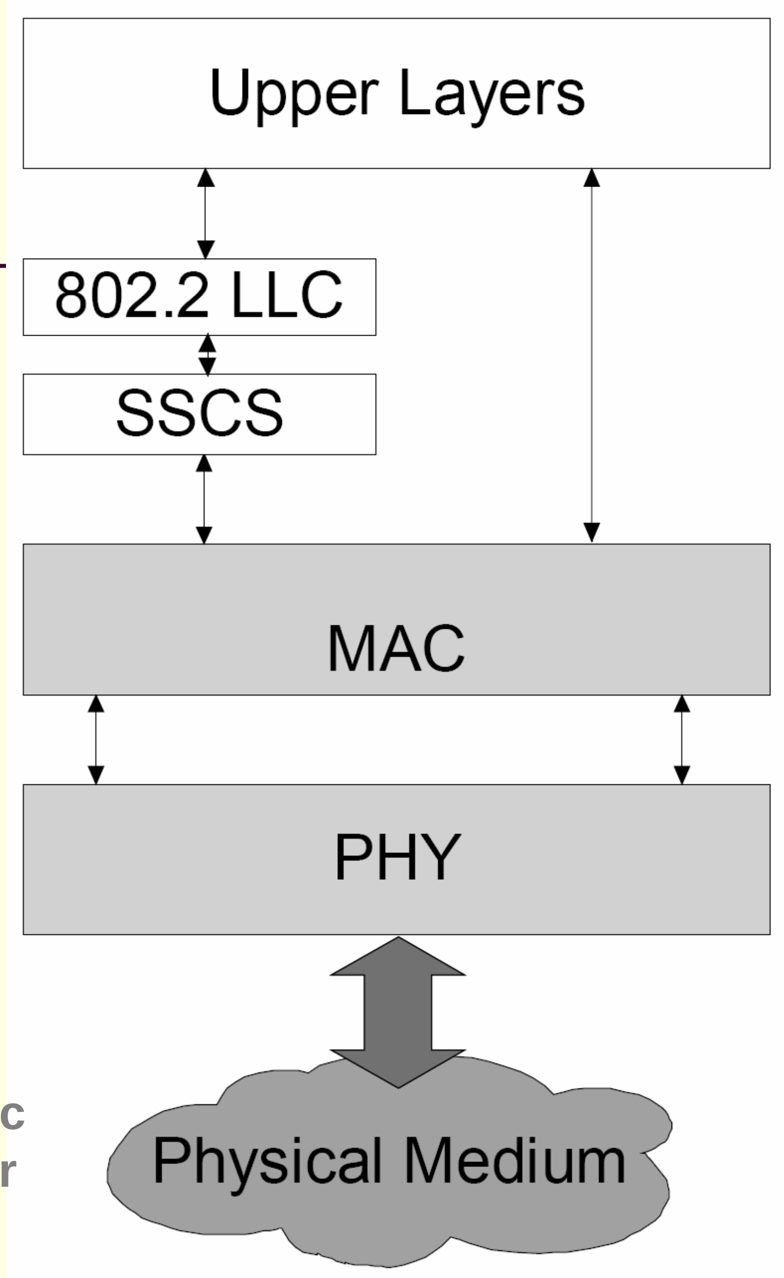
Peer-to-Peer Formation

- A cluster-tree topology

Most devices are FFD.
Any FFD can be a coordinator.
Only one PAN coordinator.
Pan coordinator forms 1st cluster (CID=0).



Protocol Architecture



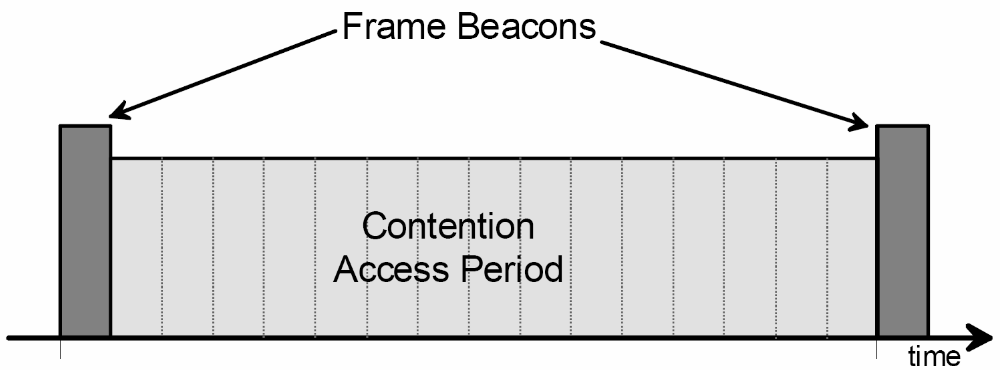
SSCS: Service Specific Convergence Sublayer

Synchronization by Superframe

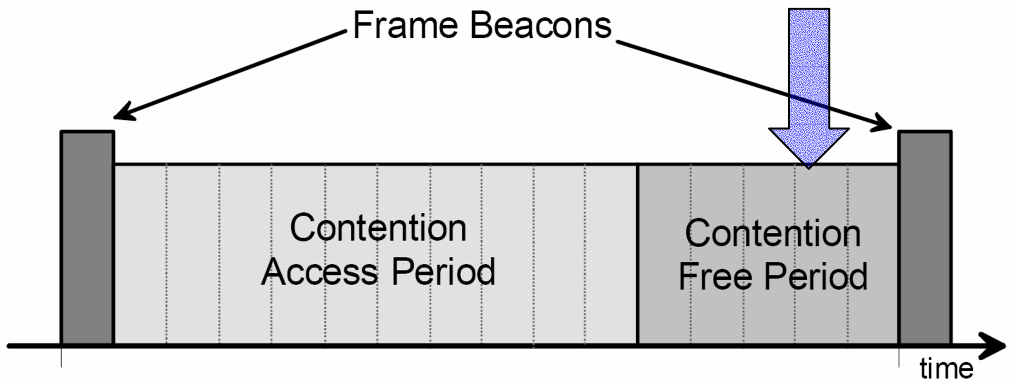
- An optional choice for the network coordinator
- A superframe is bounded by beacons sent by a coordinator.
- Between two beacons the time is divided into 15 equally sized slots.
- All the attached devices will compete the channel using a slotted CSMA/CA method.
- All transmissions shall be terminated before the next beacon.

QoS by Superframe

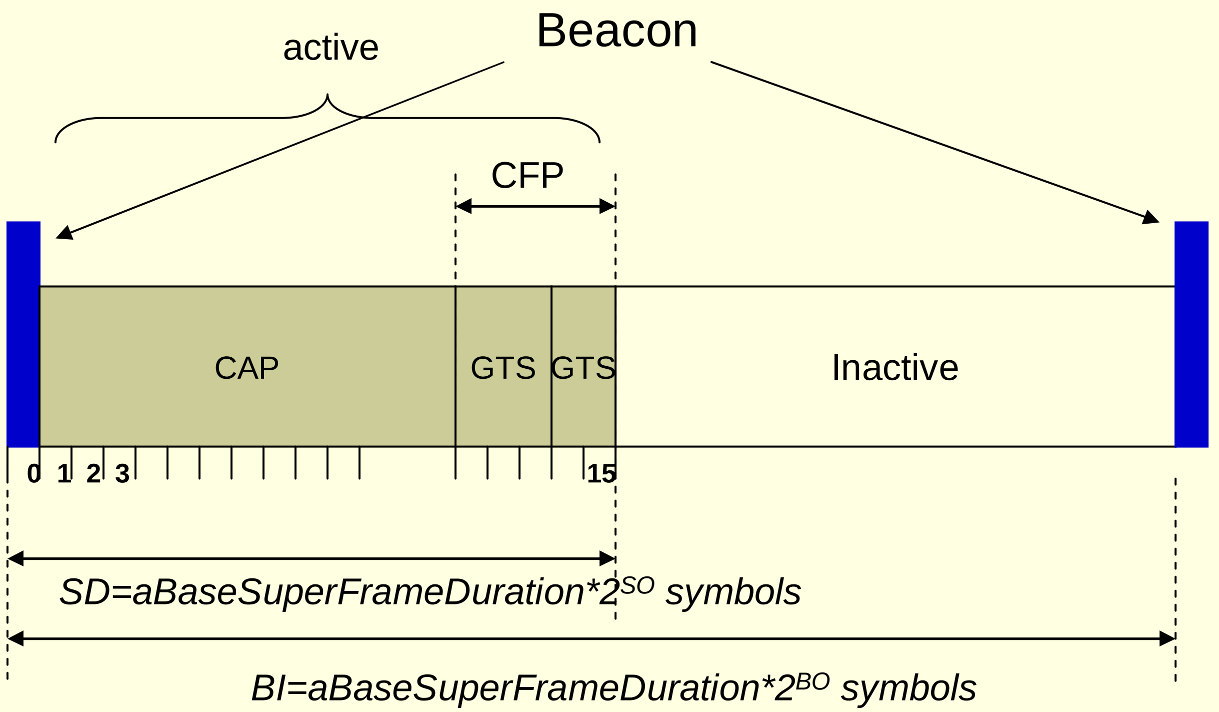
- A coordinator may reserve some time slots as Guaranteed Time Slots (GTS).
- GTSs form contention-free period (CFP), which is always behind contention access period (CAP).



Maximum up to 7 slots for GTS



Superframe with Energy Saving



SO and BO are defined as MAC attributes, 0<=SO<=BO<=14

Physical Layer: Frequency & Channels

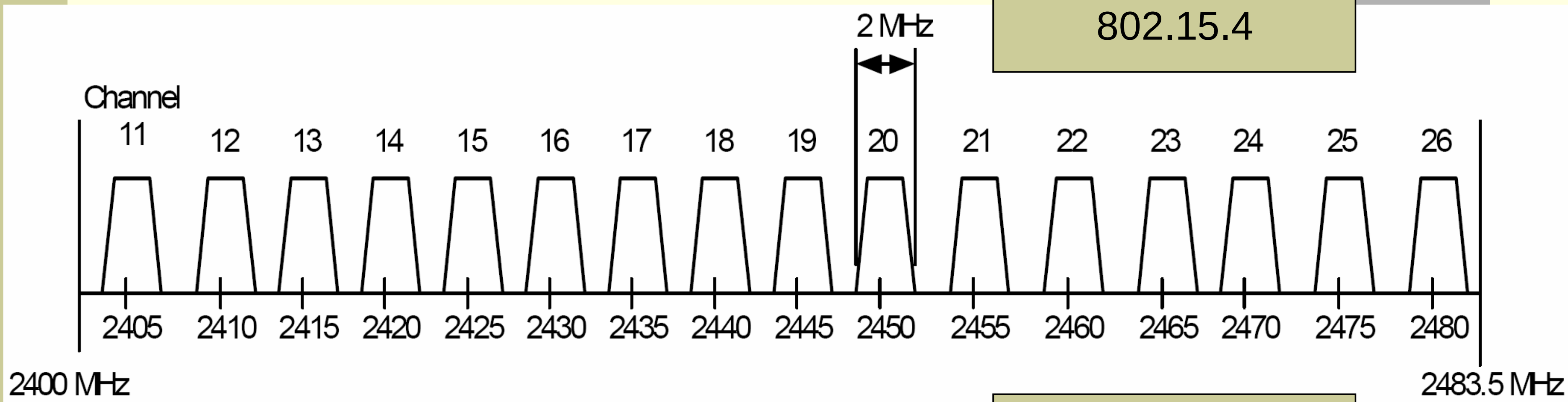
- A total of 27 channels, numbered 0 to 26, are available across the three frequency bands. 16 channels are available in the 2450 MHz band, 10 in the 915 MHz band, and 1 in the 868 MHz band.
- The center frequency of these channels is defined as follows:

$$F_c = 868.3 \qquad F_c = 906 + 2\,(k - 1) \qquad F_c = 2405 + 5\,(k - 11)$$

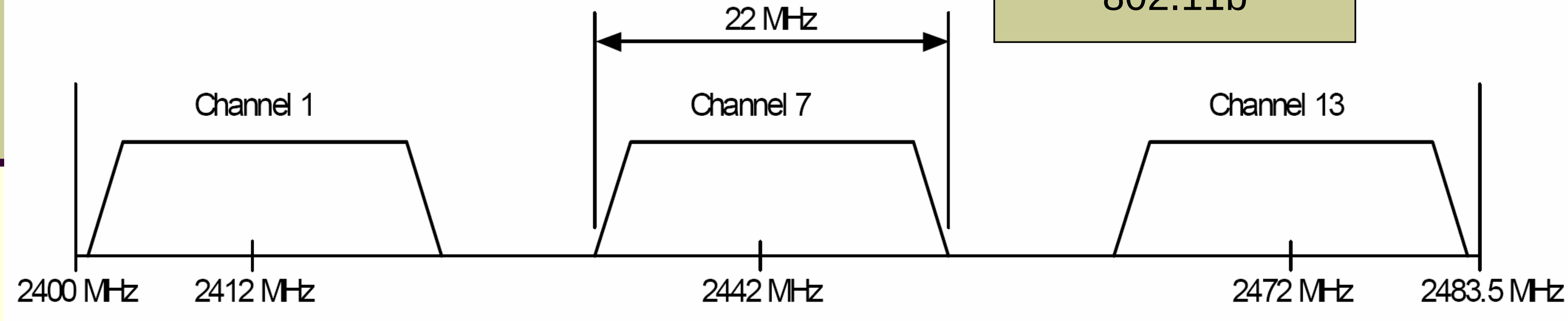
PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Channlization and Spectrum Spacing

802.15.4



802.11b



PHY Frame format

- Preamble: 32 zeros to obtain synchronization
- The start of frame delimiter (SFD): (11100101)

Bytes: 4	Bytes: 1	Bytes: 1		Bytes: variable
Preamble	Start of frame delimiter (SFD)	Frame length (7 bits)	Reserved (1 bit)	Payload
SHR		PHR		PHY payload

Frame length values	Payload
0–4	Reserved
5	MPDU (Acknowledgment)
6–7	Reserved
8 to *aMaxPHYPacketSize*	MPDU

SHR: Synchronization Header
PHR: Physical Layer Frame Header

PHY Primitives

- 3 primitives are defined between physical layer and MAC layer:
  - PD-DATA.request
  - PD-DATA.confrim
  - PD-DATA.indication
- In PD-DATA.indication a ppduLinkQuality indicator is defined as one byte (0-255), which is measured when the PPDU is received.

More Physical Layer Primitives are not discussed here.

PHY Constants

Constant	Description	Value
aMaxPHYPacketSize	The maximum PSDU size (in octets) the PHY shall be able to receive.	127
aTurnaroundTime	RX-to-TX or TX-to-RX maximum turnaround time (see 6.7.1 and 6.7.2)	12 symbol periods

PHY PIB Attributes

Attribute	Identifier	Type	Range	Description
phyCurrentChannel	0 x 00	Integer	0–26	The RF channel to use for all following transmissions and receptions (see 6.1.2).
phyChannelsSupported	0 x 01	Bitmap	See description	The 5 most significant bits (MSBs) (b_{27},... , b_{31}) of *phyChannelsSupported* shall be reserved and set to 0, and the 27 LSBs (b_0, b_1, ... b_{26}) shall indicate the status (1=available, 0=unavailable) for each of the 27 valid channels (b_k shall indicate the status of channel *k* as in 6.1.2).
phyTransmitPower	0 x 02	Bitmap	0 x 00–0xbf	The 2 MSBs represent the tolerance on the transmit power: 00 = ± 1 dB 01 = ± 3 dB 10 = ± 6 dB The 6 LSBs represent a signed integer in twos-complement format, corresponding to the nominal transmit power of the device in decibels relative to 1 mW. The lowest value of *phyTransmitPower* shall be interpreted as less than or equal to –32 dBm.
phyCCAMode	0 x 03	Integer	1–3	The CCA mode (see 6.7.9).

PIB: PAN Information Base

Coding and Modulation at 2.4G

- Every 4 bits are mapped into one symbol and encoded into one of 16 32-bit quasi-orthogonal PN codes.
- Modulation is O-QPSK

Data symbol (decimal)	Data symbol (binary) (b_0, b_1, b_2, b_3)	Chip values (c_0 c_1 ... c_{30} c_{31})
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

Pulse Shaping

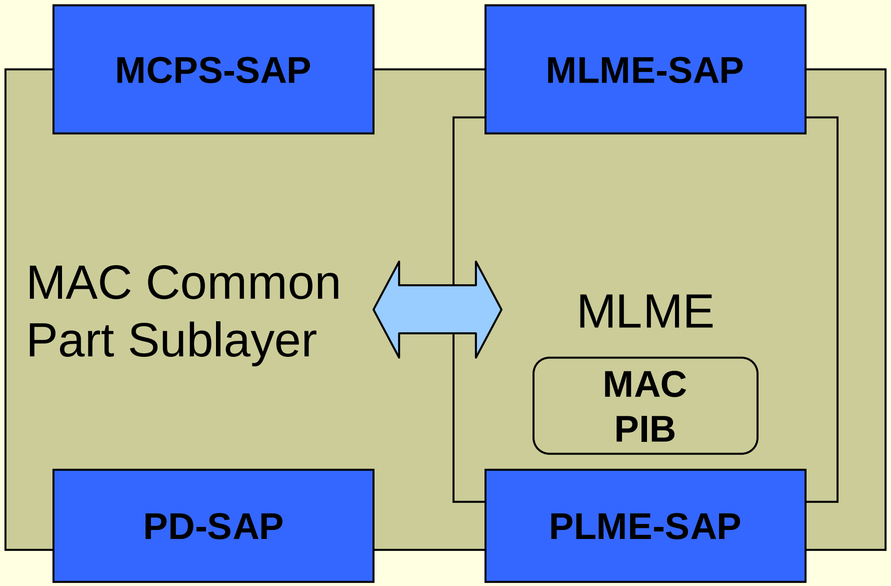
- The half-sine pulse shape used to represent each baseband chip

$$p(t) = \begin{cases} \sin\left(\pi \frac{t}{2T_c}\right), 0 \le t \le 2T_c \\ 0, otherwise \end{cases}$$

MAC Protocols

MAC Layer

- Supports two types of network topologies: star topology and peer-to-peer topology
- Any full-function device (FFD) can create its own network by becoming a PAN coordinator.
- Reduced-function devices (RFD) are coordinated by a coordinator.



MLME: MAC Layer Management Entity
PLME: Physical Layer …
MCPS: MAC Common Part Sublayer

MAC: Frame Format

- General format

Length dependent on frame control

ITU-T CRC-16

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	FCS
		Addressing fields					
MHR						MAC payload	MFR

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

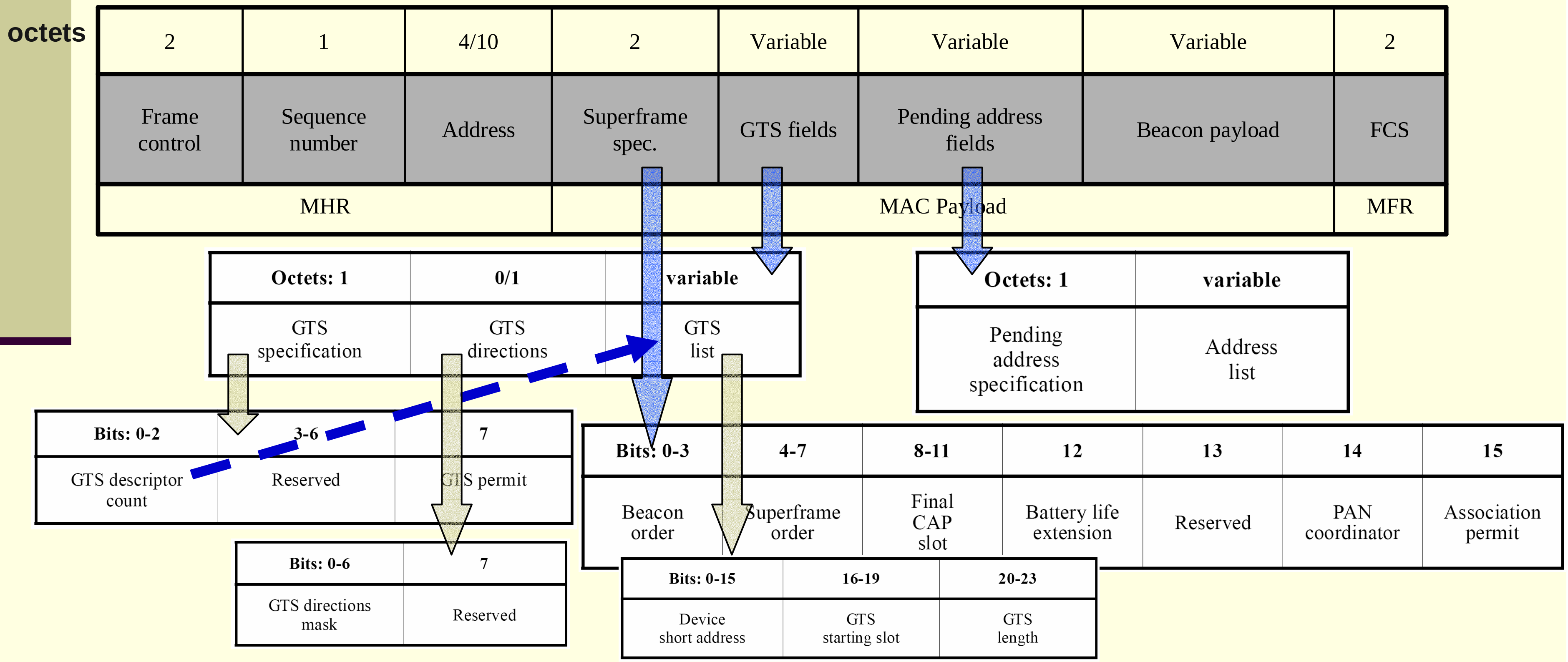
Frame type value $b_2\ b_1\ b_0$	Description
000	Beacon
001	Data
010	Acknowledgment
011	MAC command
100–111	Reserved

Frame Types

- MAC layer packet defines 4 different frame types:
  - Beacon frame
  - Data frame
  - Acknowledgement frame
  - MAC command frame

Beacon Frame

- Transmitted by coordinators periodically.
- Offers synchronization to the network.
- To identify the network and its structure.



Data & Ack. Frame

2	1	*	Variable	2
Frame control	Sequence number	Address	Data Payload	FCS
MHR			MAC Payload	MFR

2	1	1
Frame control	Sequence number	FCS
MHR		MFR

Command Frame

- Used for communication and negotiation between MAC entities on different devices.

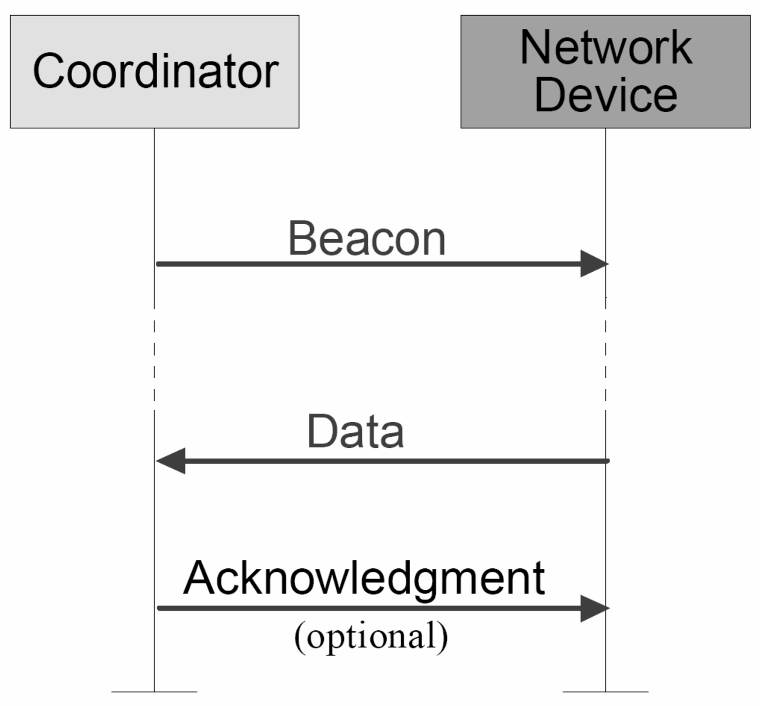
2	1	*	1	Variable	2
Frame control	Sequence number	Address	Command Frame ID	Command Payload	FCS
MHR			MAC Payload		MFR

Command frame identifier	Command name	RFD	
		Tx	Rx
0 x 01	Association request	X	
0 x 02	Association response		X
0 x 03	Disassociation notification	X	X
0 x 04	Data request	X	
0 x 05	PAN ID conflict notification	X	
0 x 06	Orphan notification	X	
0 x 07	Beacon request		
0 x 08	Coordinator realignment		X
0 x 09	GTS request		
0 x 0a—0 x ff	Reserved		

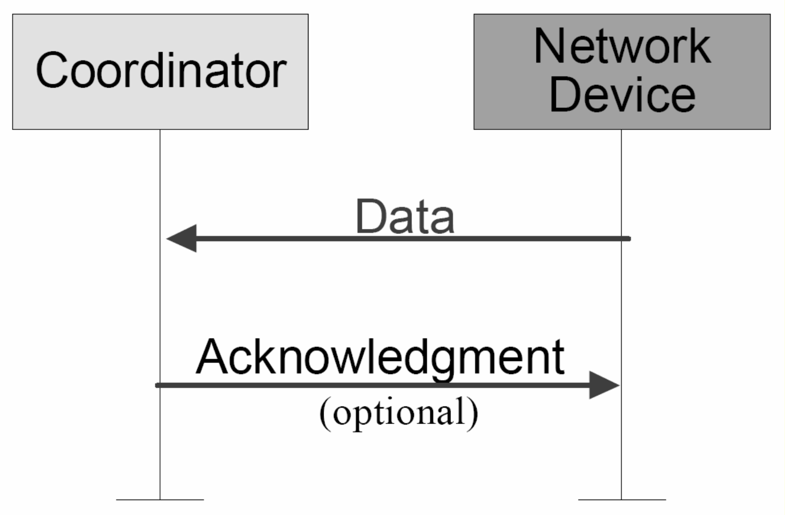
Data Transfer

- Data from a device to a coordinator
- Data from a coordinator to a device
- Data from a device to a device (peer-to-peer)

Device to Coordinator

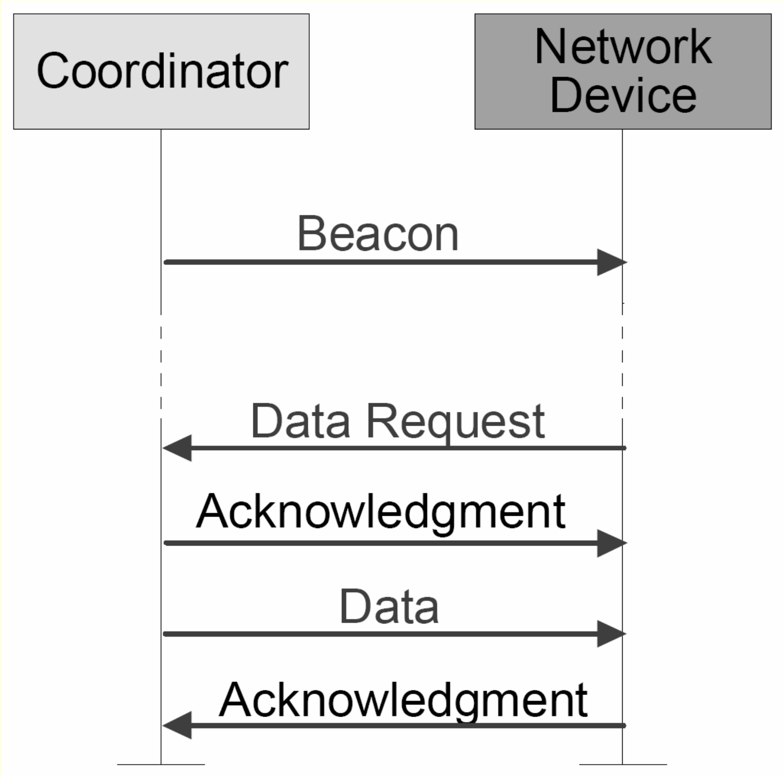


Communication to a coordinator in a beacon-enabled network

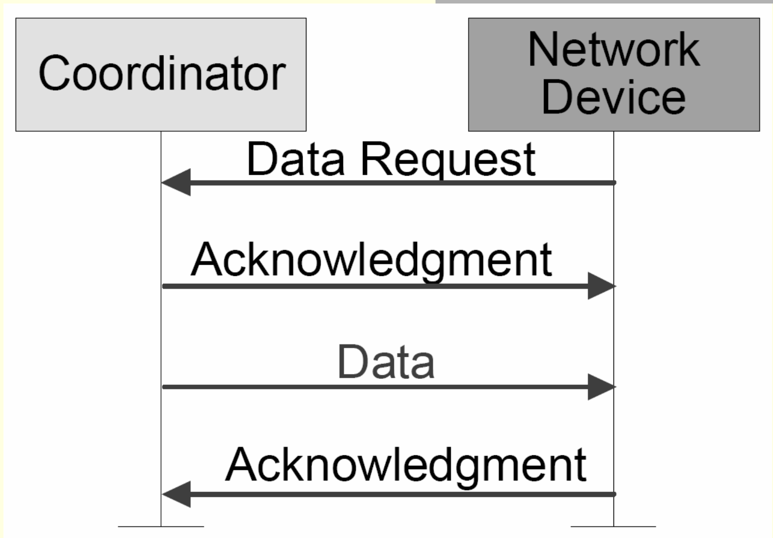


Communication to a coordinator in a nonbeacon-enabled network

Coordinator to Device



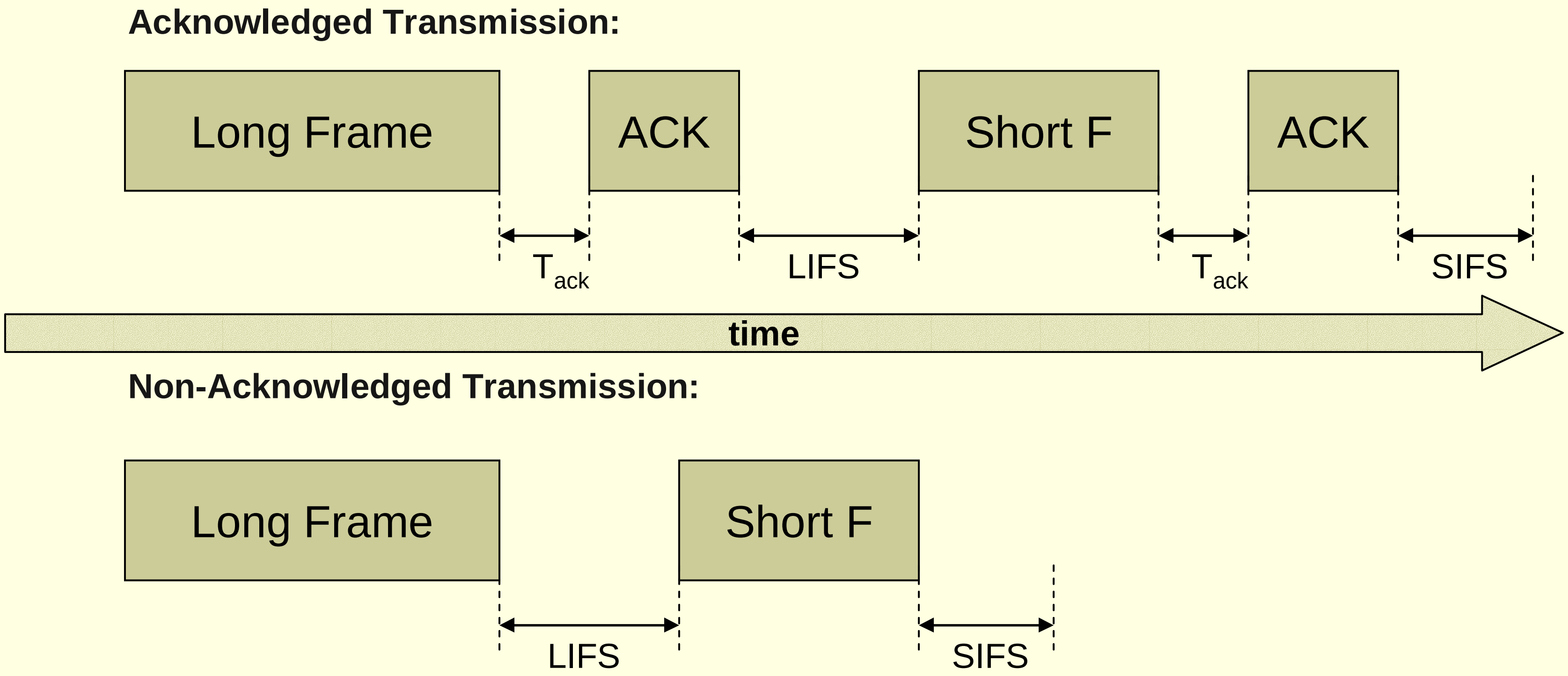
Communication from a coordinator in a beacon-enabled network



Communication from a coordinator in a nonbeacon-enabled network

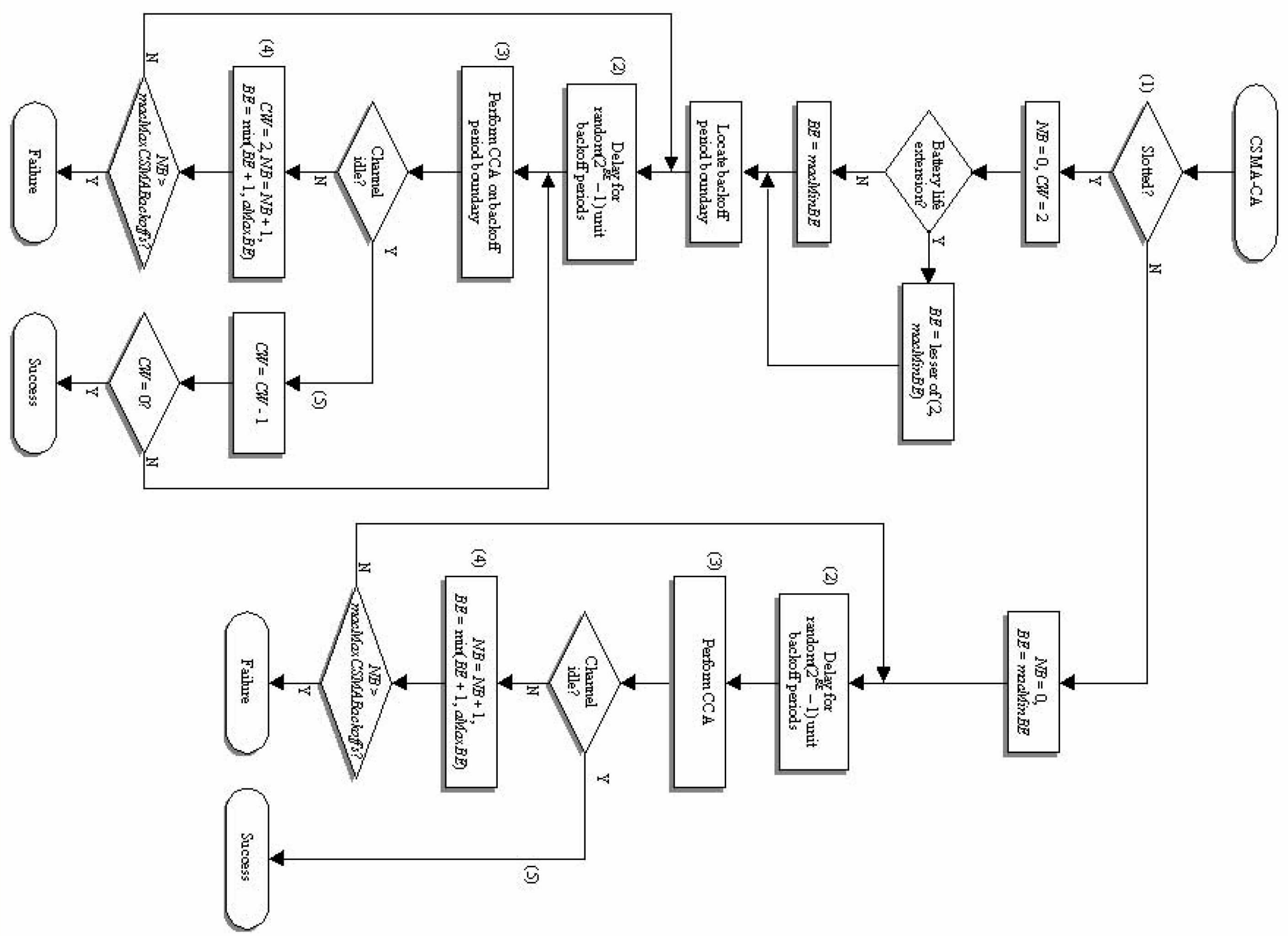
MAC: IFS

- Inter-Frame Space



$aTurnaroundTime <= T_{ack} <= (aTurnaroundTime + aUnitBackoffPeriod)$

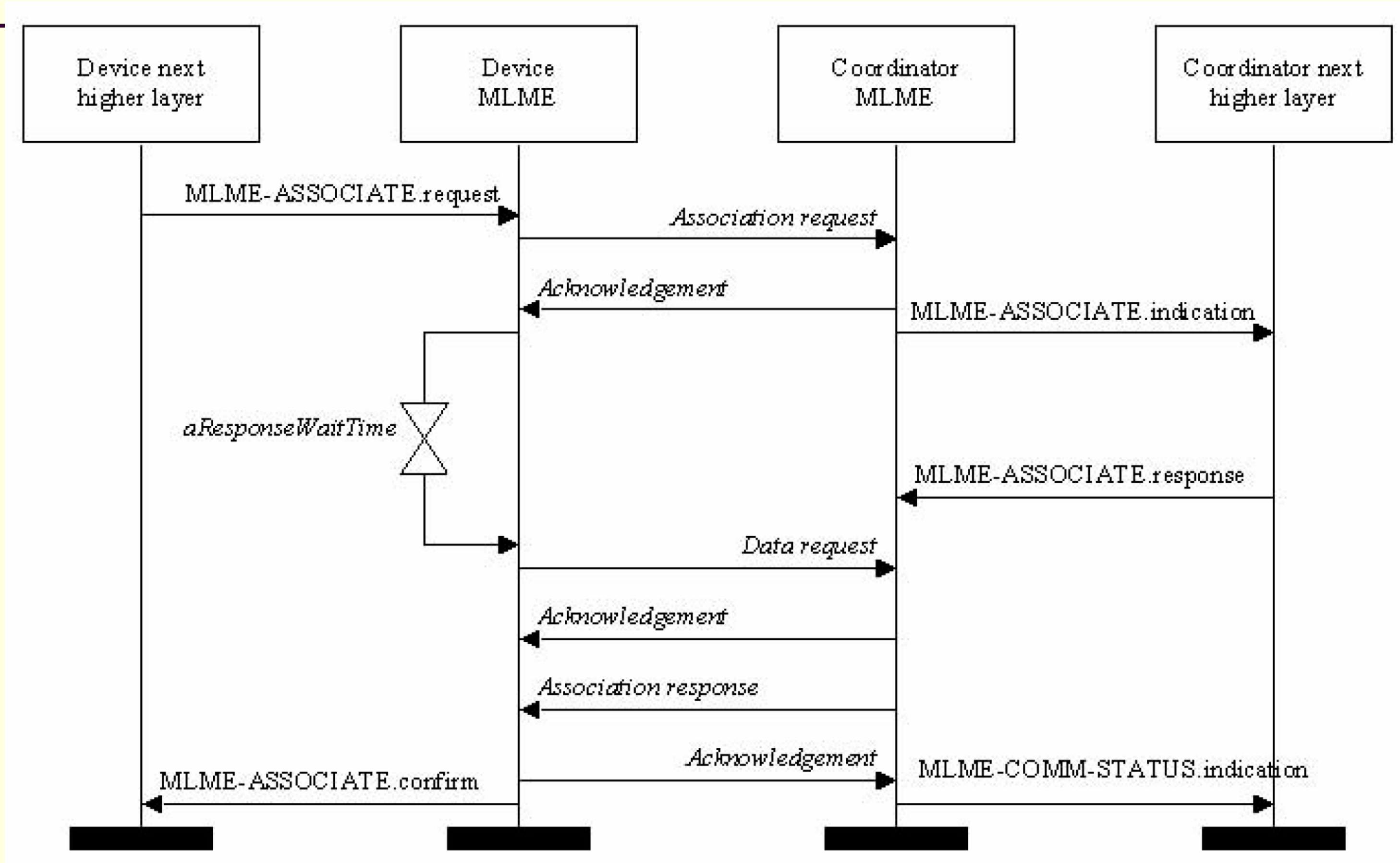
Slotted CSMA/CA



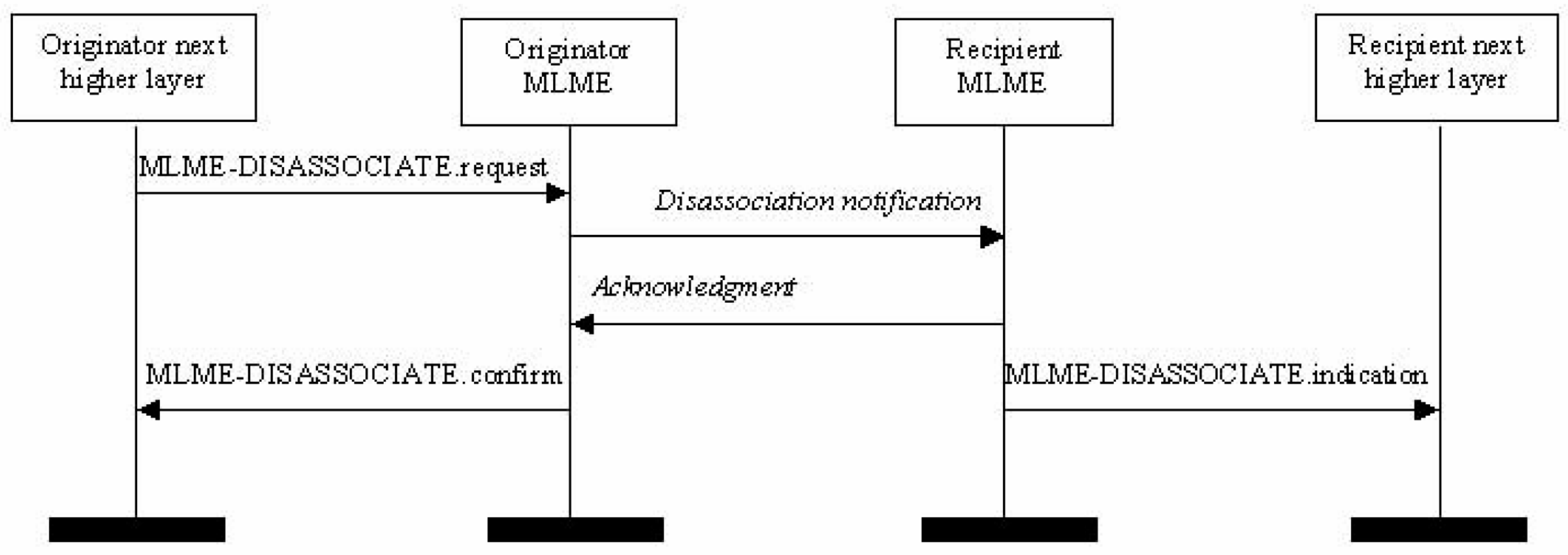
Communication in P2P Network

- In a peer-to-peer PAN, every device may communicate with every other device in its radio sphere of influence.
- In order to do this effectively, the devices wishing to communicate will need to either receive constantly or synchronize with each other.
- In the former case, **the device can simply transmit its data using unslotted CSMA-CA**.
- In the latter case, other measures need to be taken in order to achieve synchronization.
- **Such measures are beyond the scope of this standard.**

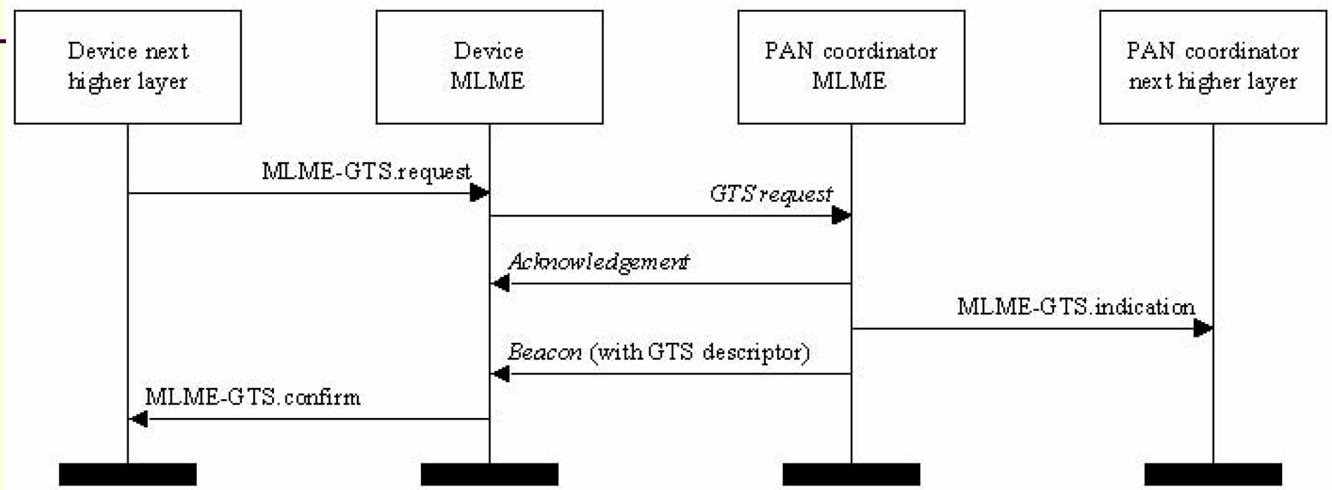
MAC: Device Association

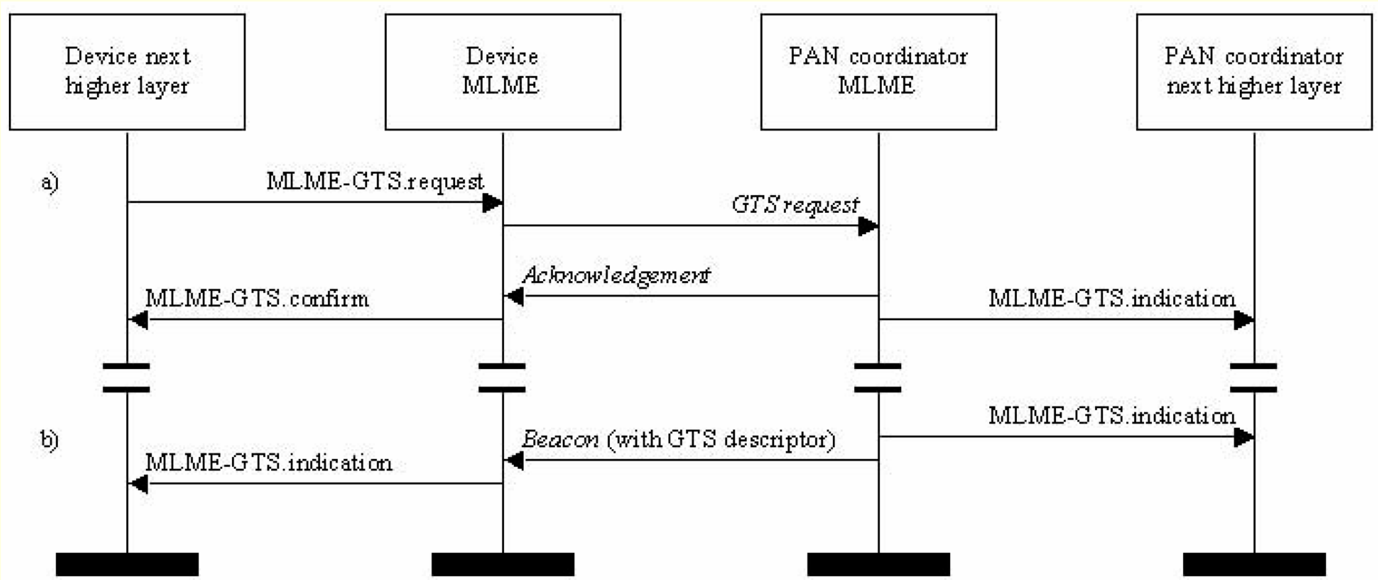


MAC: Device Disassociation

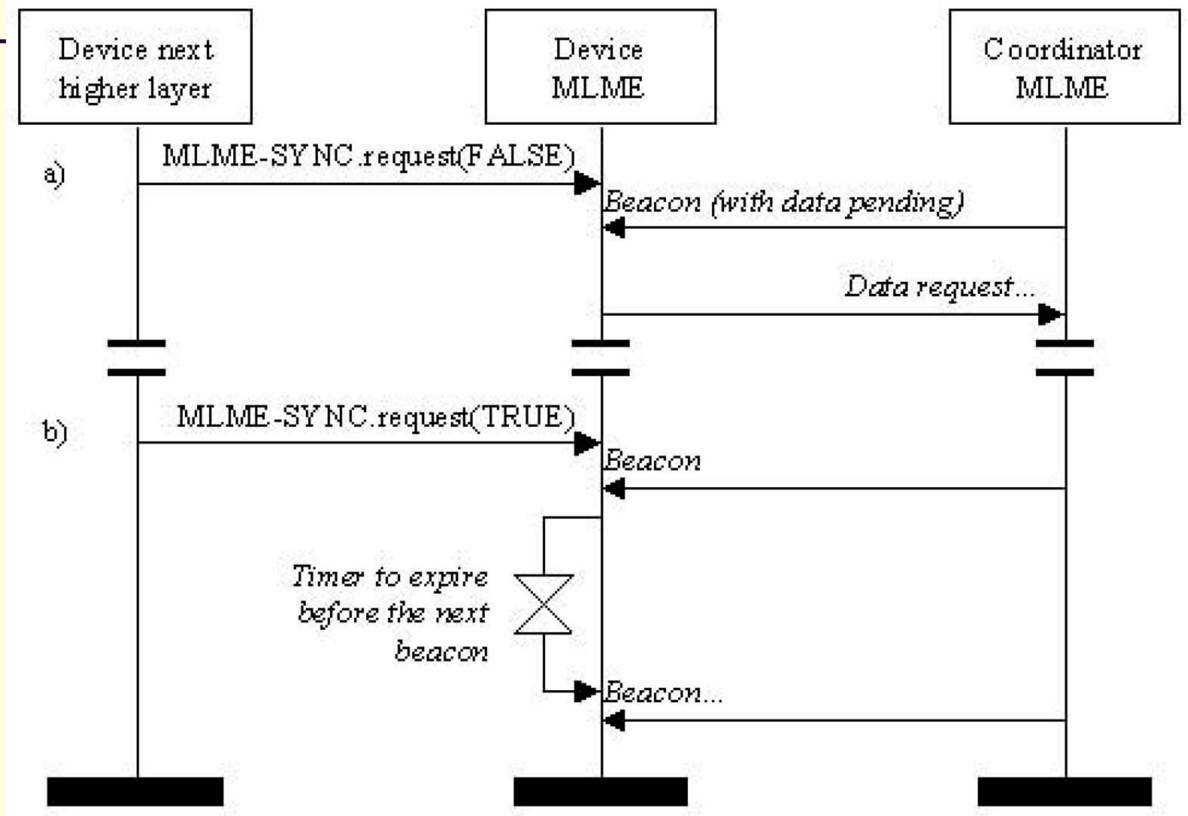


MAC: GTS Allocation/Deallocation



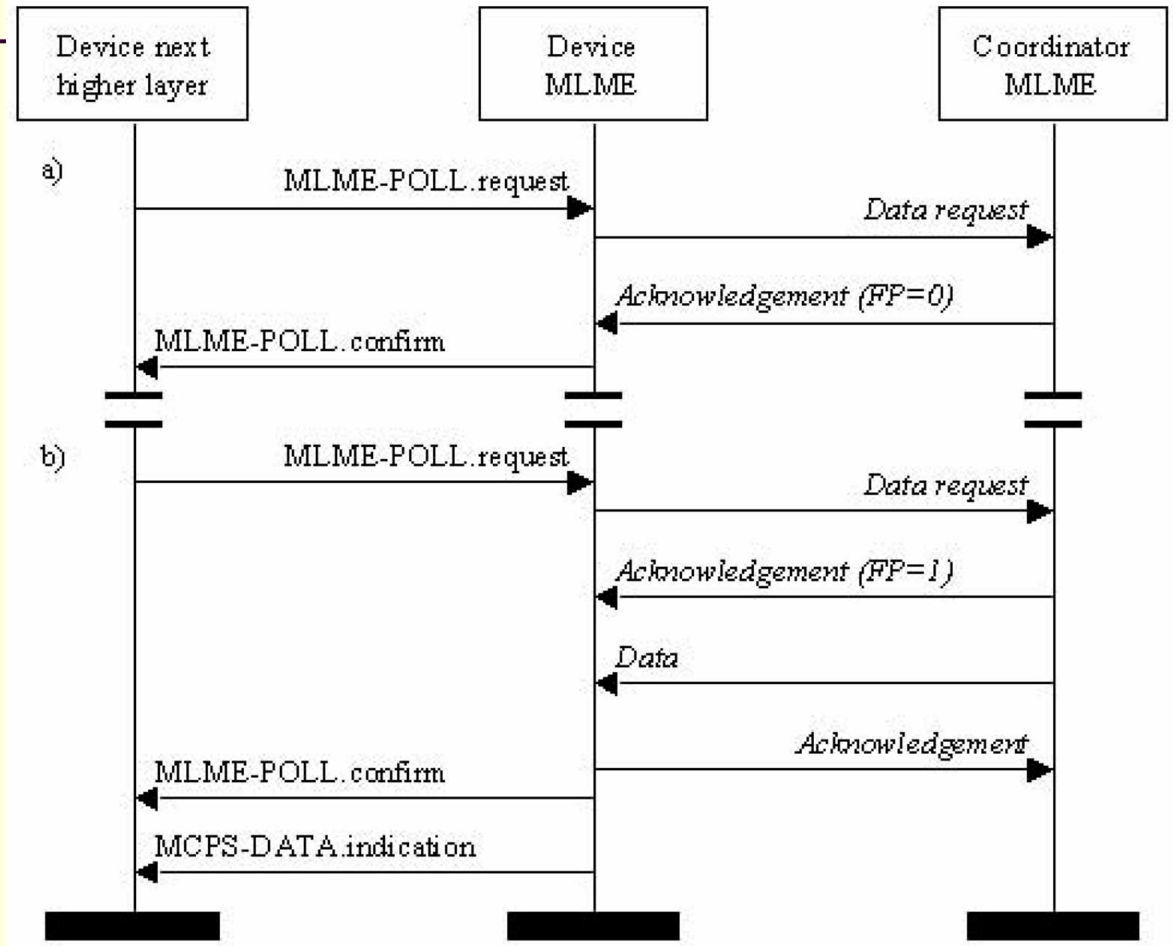


MAC: Device Synchronization



a) **A single synchronization**
b) **Track synchronization**

MAC: Polling from Coordinator



a) **No data pending**
b) **Has data pending to the device**

MAC PIB Constants

Constant	Description	Value
aBaseSlotDuration	The number of symbols forming a superframe slot when the superframe order is equal to 0.	60
aBaseSuperframeDuration	The number of symbols forming a superframe when the superframe order is equal to 0.	*aBaseSlotDuration* * aNumSuperframeSlots
aExtendedAddress	The 64 bit (IEEE) address assigned to the device.	Device specific
aMaxBE	The maximum value of the backoff exponent in the CSMA-CA algorithm.	5
aMaxBeaconOverhead	The maximum number of octets added by the MAC sublayer to the payload of its beacon frame.	75
aMaxBeaconPayloadLength	The maximum size, in octets, of a beacon payload.	*aMaxPHYPacketSize – aMaxBeaconOverhead*
aGTSDescPersistenceTime	The number of superframes in which a GTS descriptor exists in the beacon frame of a PAN coordinator.	4
aMaxFrameOverhead	The maximum number of octets added by the MAC sublayer to its payload without security. If security is required on a frame, its secure processing may inflate the frame length so that it is greater than this value. In this case, an error is generated through the appropriate .confirm or MLME-COMM-STATUS.indication primitives.	25
aMaxFrameResponseTime	The maximum number of CAP symbols in a beacon-enabled PAN, or symbols in a nonbeacon-enabled PAN, to wait for a frame intended as a response to a data request frame.	1220
aMaxFrameRetries	The maximum number of retries allowed after a transmission failure.	3
aMaxLostBeacons	The number of consecutive lost beacons that will cause the MAC sublayer of a receiving device to declare a loss of synchronization.	4
aMaxMACFrameSize	The maximum number of octets that can be transmitted in the MAC frame payload field.	*aMaxPHYPacketSize – aMaxFrameOverhead*
aMaxSIFSFrameSize	The maximum size of an MPDU, in octets, that can be followed by a short interframe spacing (SIFS) period.	18
aMinCAPLength	The minimum number of symbols forming the CAP. This ensures that MAC commands can still be transferred to devices when GTSs are being used. An exception to this minimum shall be allowed for the accommodation of the temporary increase in the beacon frame length needed to perform GTS maintenance (see 7.2.2.1.3).	440
aMinLIFSPeriod	The minimum number of symbols forming a long interframe spacing (LIFS) period.	40
aMinSIFSPeriod	The minimum number of symbols forming a SIFS period.	12
aNumSuperframeSlots	The number of slots contained in any superframe.	16
aResponseWaitTime	The maximum number of symbols a device shall wait for a response command to be available following a request command.	32 * *aBaseSuperframeDuration*
aUnitBackoffPeriod	The number of symbols forming the basic time period used by the CSMA-CA algorithm.	20

Elements of ACL Entry Descriptor

Name	Type	Range	Description	Default
ACLExtendedAddress	IEEE address	Any valid 64 bit device address	The 64 bit IEEE extended address of the device in this ACL entry.	Device specific
ACLShortAddress	Integer	0 x 0000–0 x ffff	The 16 bit short address of the device in this ACL entry. A value of 0 x fffe indicates that the device is using only its 64 bit extended address. A value of 0 x ffff indicates that this value is unknown.	0 x ffff
ACLPANId	Integer	0 x 0000–0 x ffff	The 16 bit PAN identifier of the device in this ACL entry.	Device specific
ACLSecurityMaterial-Length	Integer	0–26	The number of octets contained in *ACL-SecurityMaterial*.	21
ACLSecurityMaterial	Octet string	Variable	The specific keying material to be used to protect frames between the MAC sublayer and the device indicated by the associated *ACLExtendedAddress* (see 7.6.1.8).	Empty string
ACLSecuritySuite	Integer	0 x 00–0 x 07	The unique identifier of the security suite to be used to protect communications between the MAC sublayer and the device indicated by the associated *ACLExtendedAddress* as specified in Table 75.	0 x 00

ACL: Access Control List

Channel Scanning

- All devices shall be capable of performing passive and orphan scans across a specified list of channels.
- In addition, an FFD shall be able to perform ED (Energy Detection) and active scans.
- The next higher layer should submit a *scan request* containing a list of channels chosen only from the channels specified by *phyChannelsSupported.*

Channel Scanning: ED Scan

- Allows an FFD to obtain a measure of the peak energy in each requested channel.
- Used by a prospective PAN coordinator to select a channel in which to operate prior to starting a new PAN.
- Shall terminate when either the number of measurements stored equals the implementation-specified maximum or energy has been measured on each of the specified logical channels.

Channel Scanning: Active Channel Scan

- Allows an FFD to locate any coordinator transmitting beacon frames within its POS.
- Used by a prospective PAN coordinator to select a PAN identifier prior to starting a new PAN, or used by a device prior to association.
- A device conducting an active scan sends a *beacon-request* command.

- If a coordinator of a beacon-enabled PAN receives the beacon request command, it shall ignore the command and continue transmitting its beacons as usual.
- If a coordinator of a nonbeacon-enabled PAN receives this command, it shall transmit a single beacon frame using unslotted CSMA-CA.

Channel Scanning: Passive Channel Scan

- Allows a device to locate any coordinator transmitting beacon frames within its POS.
- The beacon request command is not transmitted.
- This type of scan could be used by a device prior to association.

Channel Scanning: Orphan Channel Scan

- Allows a device to attempt to relocate its coordinator following a loss of synchronization.

- If a coordinator receives the *orphan notification* command, it shall search its device list for the device sending the command.
- If the coordinator finds a record of the device, it shall send a *coordinator realignment* command to the orphaned device.

Synchronization

- Synchronization with beacons
- Synchronization without beacons
  - A device shall be able to poll the coordinator for data at the discretion of the next higher layer.

GTS:

- Allocation
- De-allocation
- Reallocation

GTS: Allocation

- A device is instructed to request the allocation of a new GTS through the *MLME-GTS.request* primitive.
- The coordinator sends back an ACK after the reception of GTS request command.
- GTSs shall be allocated on a first-come-first-served basis by the PAN coordinator.
- The coordinator sends the GTS descriptor in next beacon to indicate the device when the allocated GTS slot starts, how many, and the direction.

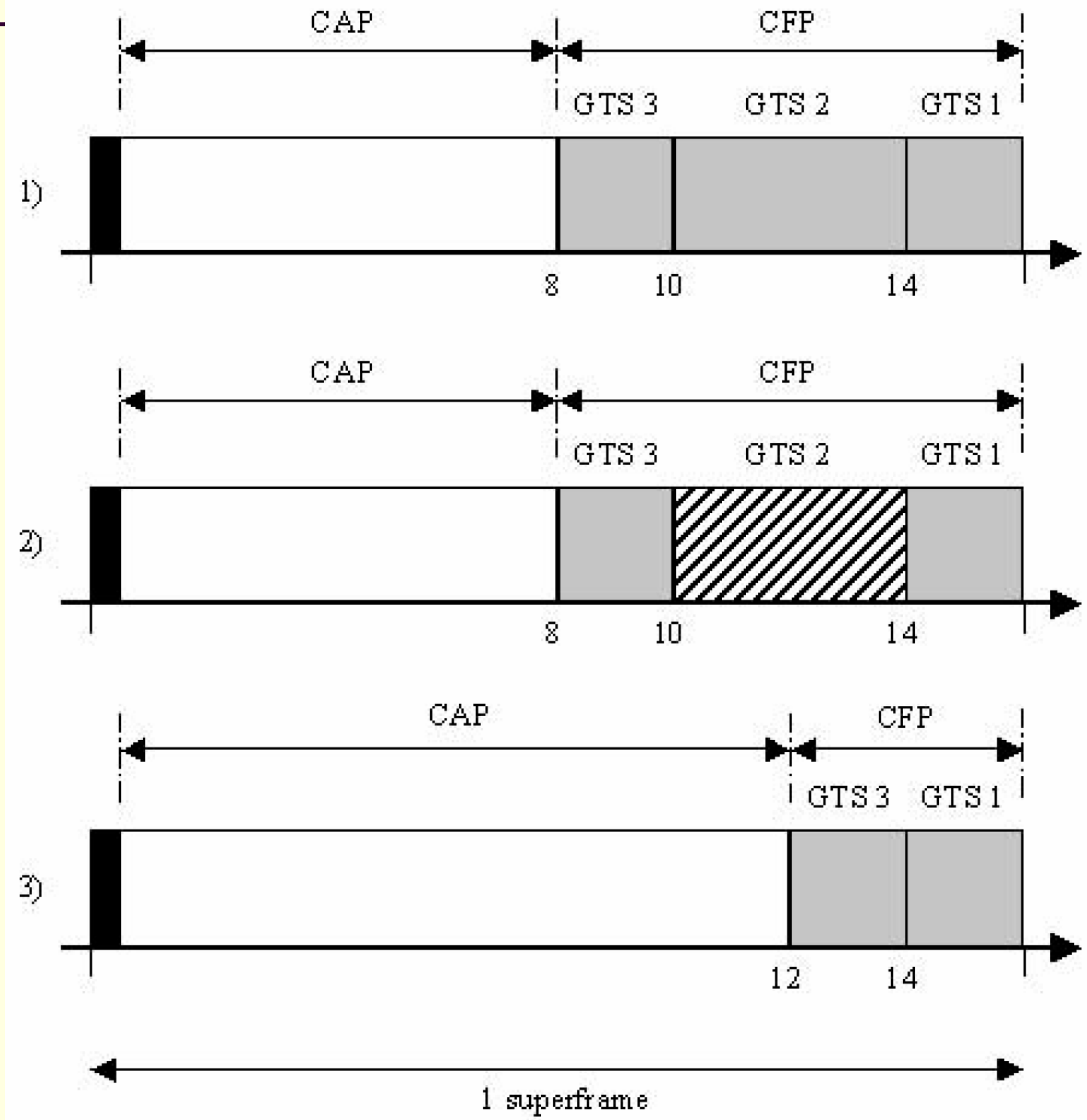
- The transaction of GTS should follow the MAC IFS limit.

GTS: De-allocation

- To request the de-allocation of an existing GTS, the MLME shall send the GTS request command to the PAN coordinator.
- The characteristics type subfield of the GTS characteristics field of the request shall be set to 0.
- This request must be acknowledged.
- On receipt of a beacon frame containing a GTS descriptor corresponding to *macShortAddress* and a start slot equal to 0, the device shall immediately stop using the GTS.

GTS: Reallocation

The PAN coordinator shall ensure that any gaps occurring in the CFP, appearing due to the de-allocation of a GTS, are removed to maximize the length of the CAP.



GTS Expiration

- The PAN coordinator shall attempt to detect when a device has stopped using a GTS using the following rules:
  - For a transmit GTS, the coordinator shall assume that a device is no longer using its GTS if a data frame is not received from the device in the GTS at least every 2**n* superframes,
  - For receive GTSs, the coordinator shall assume that a device is no longer using its GTS if an acknowledgment frame is not received from the device at least every 2**n* superframes,

$$n = 2^{(8-\mathrm{macBeaconOrder})} \qquad 0 \le \mathrm{macBeaconOrder} \le 8$$

$$n = 1 \qquad 9 \le \mathrm{macBeaconOrder} \le 14$$

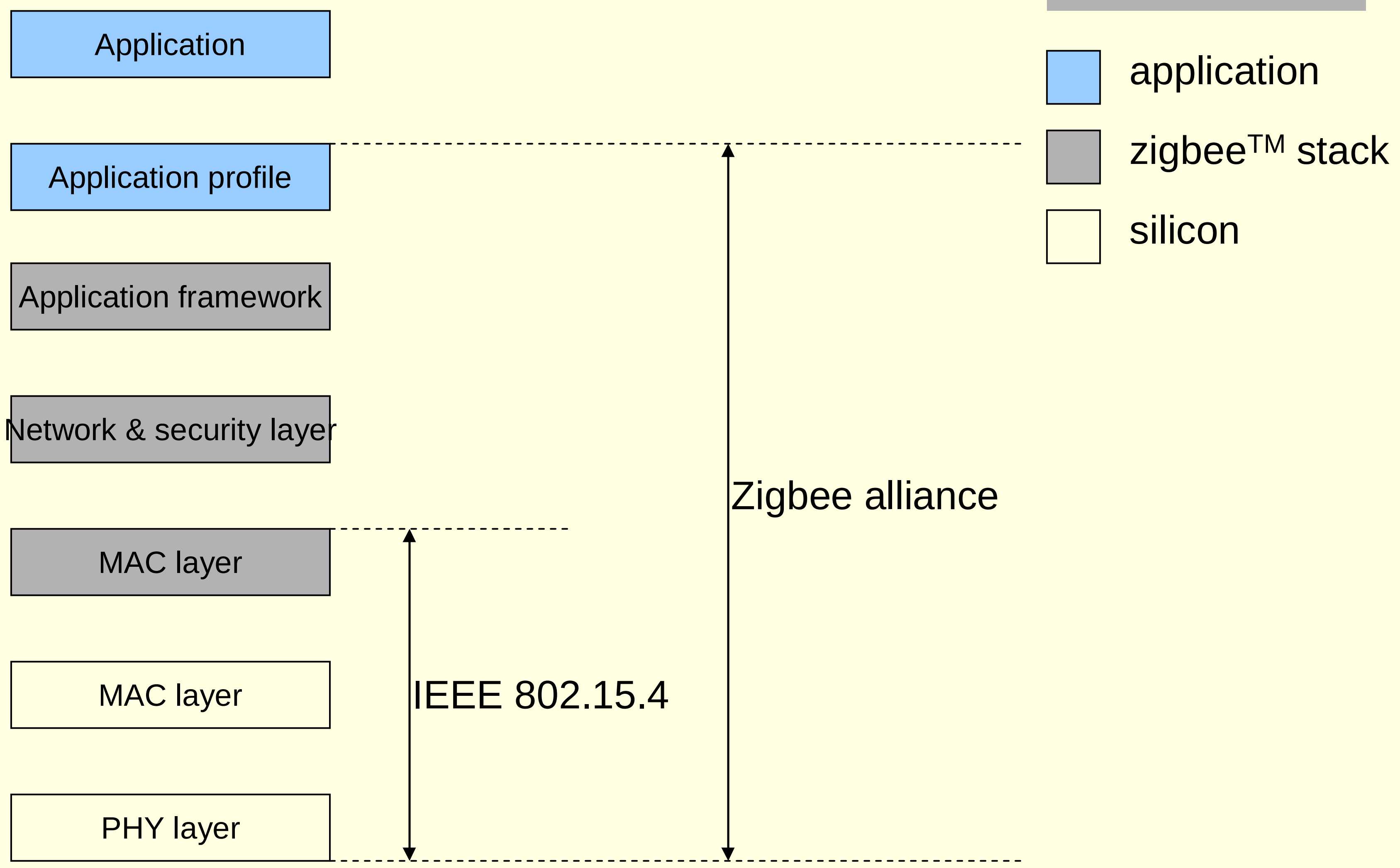
Zigbee Alliance

- A industrial alliance for developing MAC layer protocol and higher layer protocols for IEEE 802.15.4.
- Including a group of promoters and participants.

Zigbee Products

- Chipcon offers a development kit for zigbee application.
  - CC2420 - Industry leading IEEE 802.15.4/ZigBee RF transceiver
  - CC2430 - True System-on-Chip (SoC) solution for ZigBee with integrated 8051 microcontroller
  - ZigBee hardware development kits
  - High performance and robust reference designs
  - IEEE 802.15.4 MAC software free-of-charge

Development Roadmap

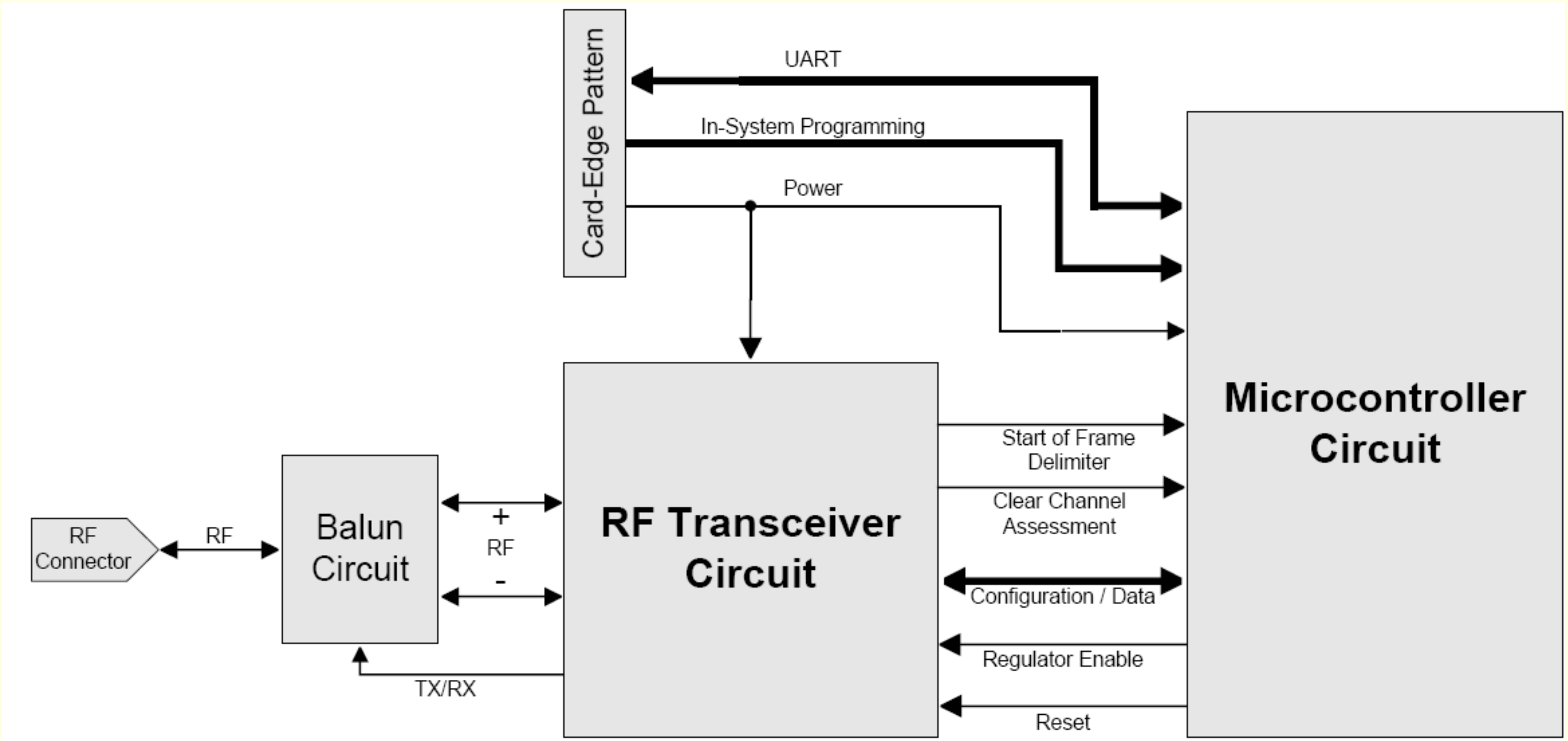


Design Example*

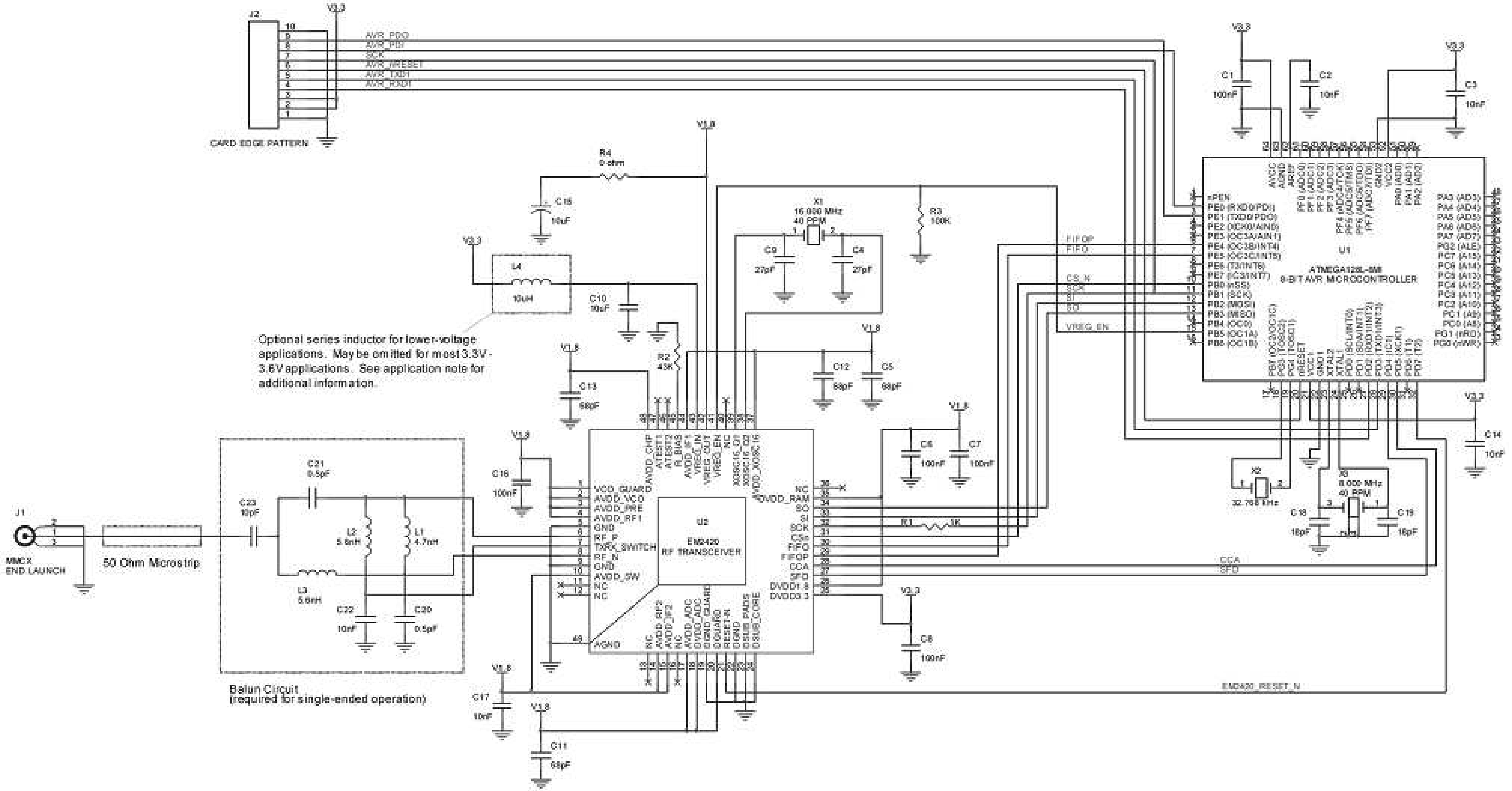
- ATMEL ATmega128L or ATmega64L 8-bit microcontroller
  - 128 or 64 kB flash memory
  - In-System Programming
  - Standard UART
- Ember EM2420 radio frequency transceiver
  - Zigbee compliant
  - 2.4GHz ISM band
  - Nominal Tx power -0.5dBm, receiver sensitivity -94dBm

*quoted from Ember application note:
http://www.ember.com/downloads/pdfs/AppNote-EM2420.pdf

Block Diagram

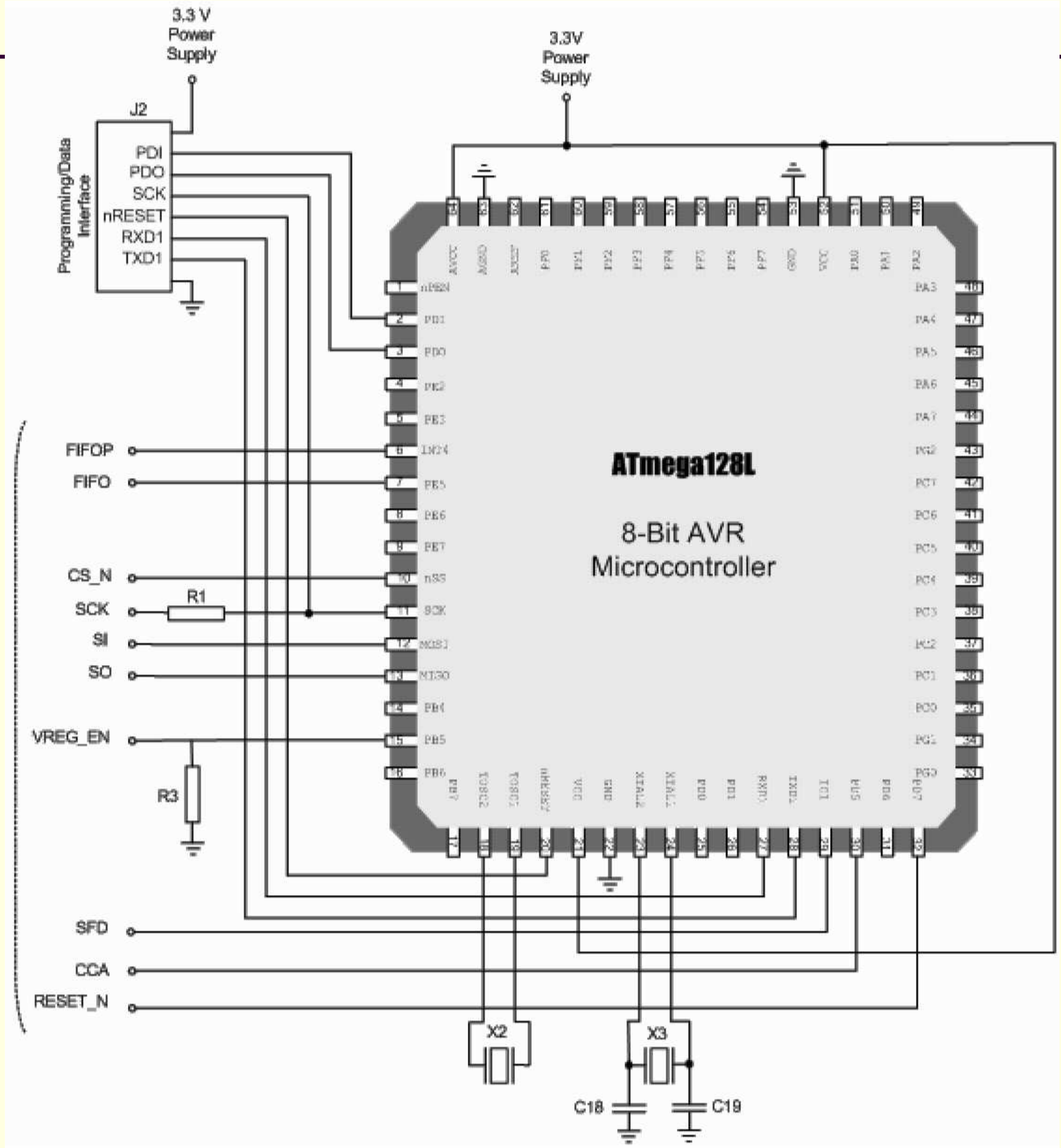


Schematic Circuitry

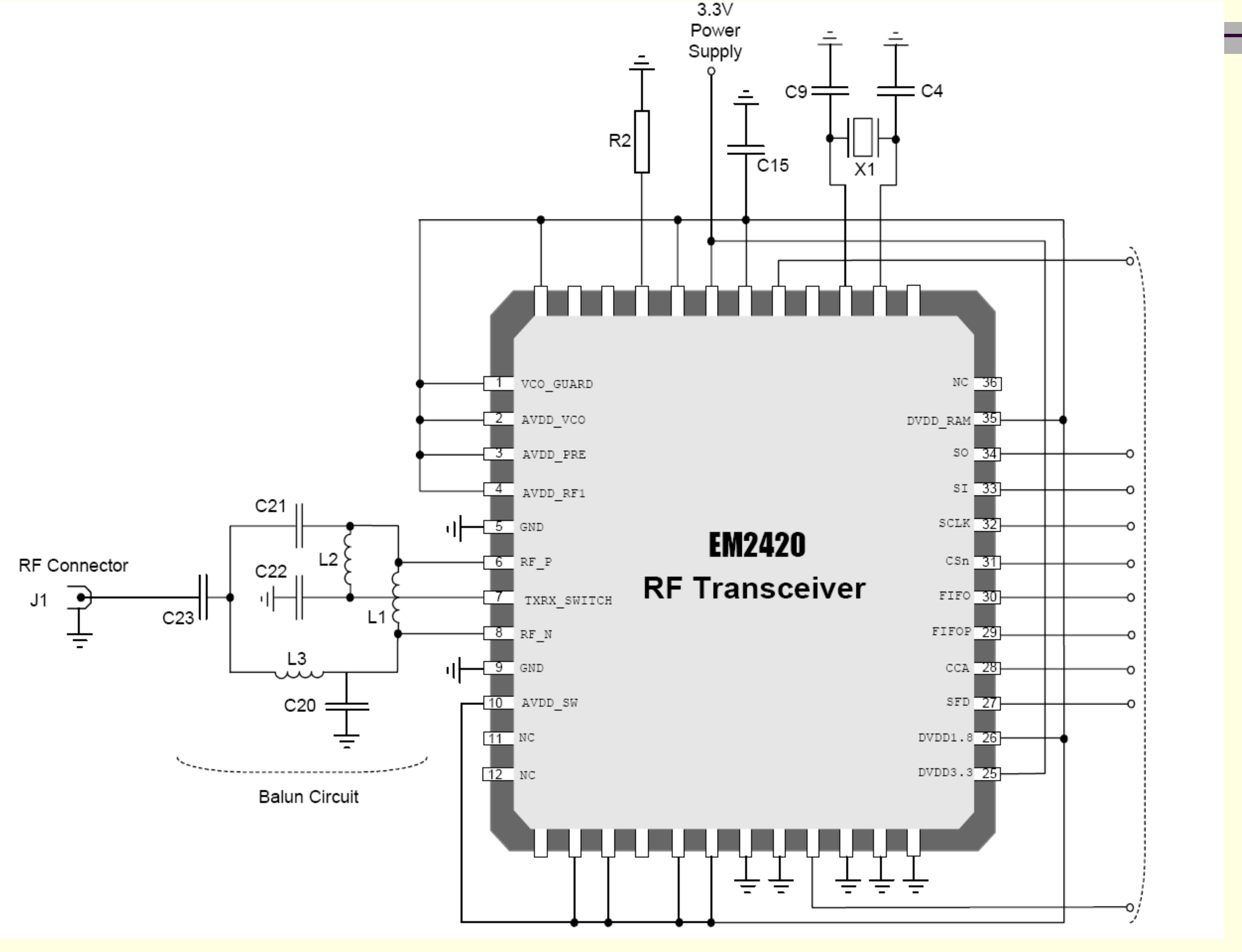


ATmegaXX configuration

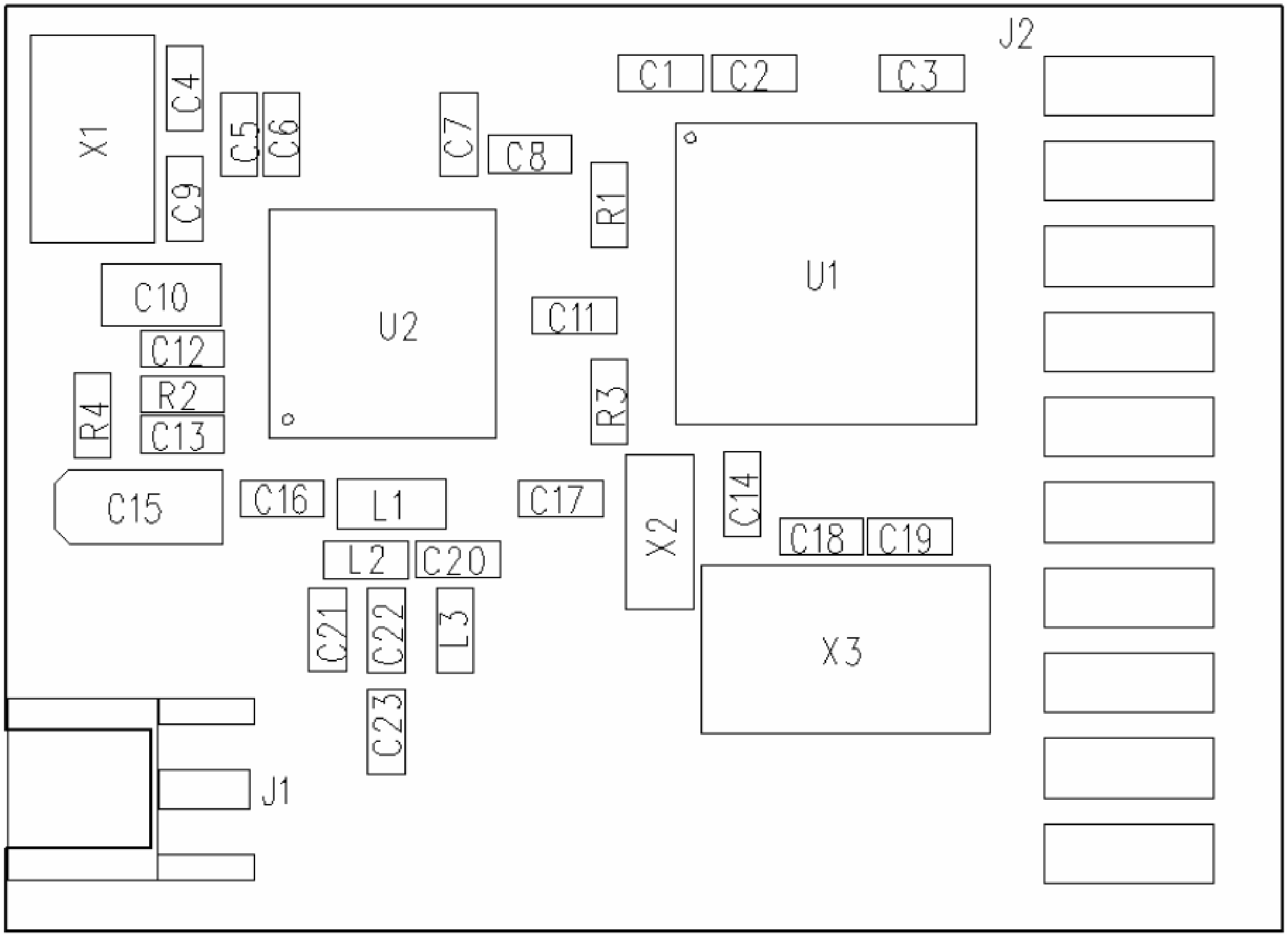
RF txr interface



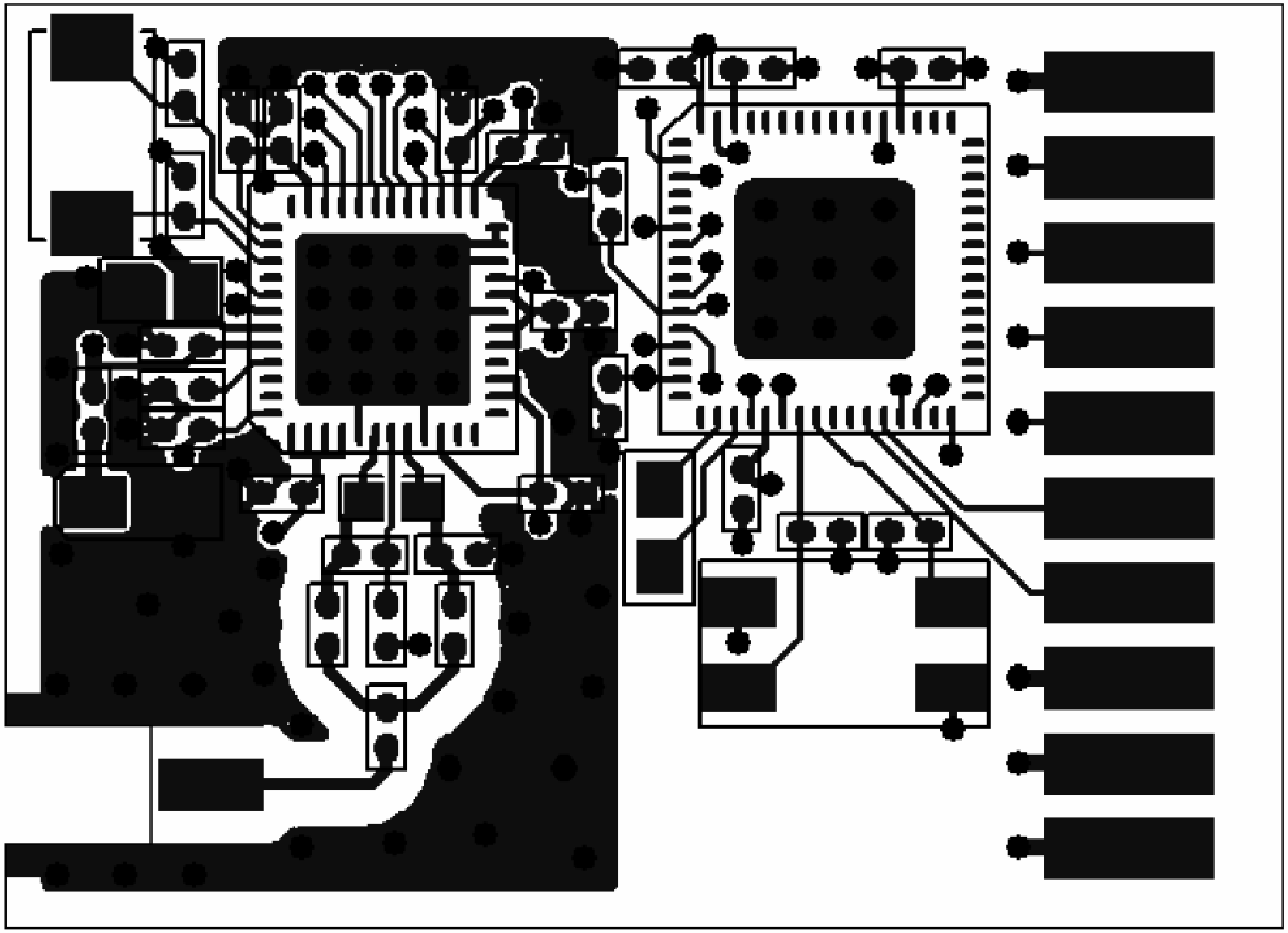
RF circuits


3.3V
Power
Supply
R2
C15
C9
C4
X1
VCO_GUARD
AVDD_VCO
AVDD_PRE
AVDD_RF1
GND
RF_P
TXRX_SWITCH
RF_N
GND
AVDD_SW
NC
NC
NC
DVDD_RAM
SO
SI
SCLK
CSn
FIFO
FIFOP
CCA
SFD
DVDD1.8
DVDD3.3
EM2420
RF Transceiver
C21
C22
L2
L1
L3
C20
C23
RF Connector
J1
Balun Circuit

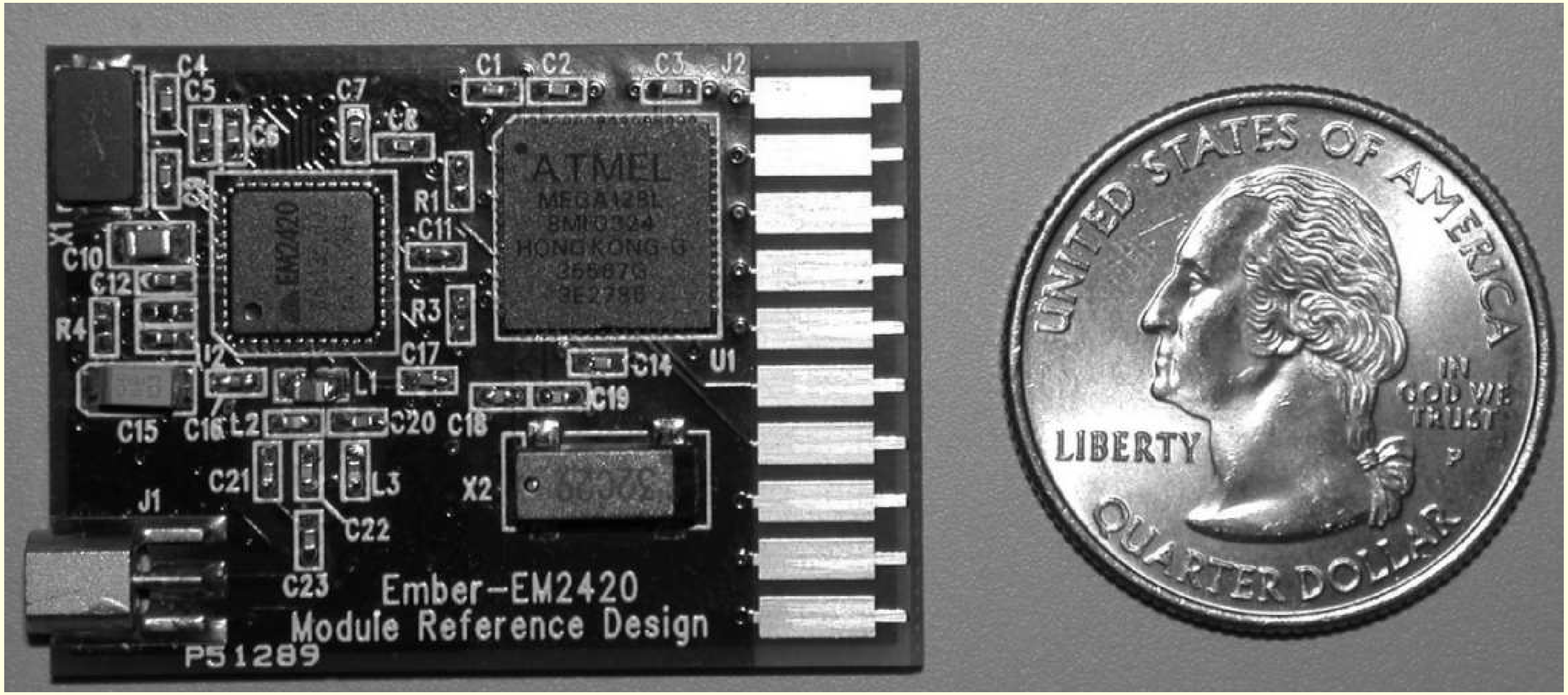
Components Placement



PCB Layout



Prototype


Ember-EM2420
Module Reference Design
P51289
ATMEL
MEGA128L
LIBERTY
IN GOD WE TRUST
UNITED STATES OF AMERICA
QUARTER DOLLAR

Conclusion

- IEEE 802.15.4 is well considered to save energy.
  - GTS
  - Active/inactive slots
  - ED
  - LQI
- Synchronization can be done locally by coordinator, but a global synchronization for a multihop peer-to-peer network is not specified (and seems difficult to be realized).
- The protocol stack is quite heavy.

Thank You!