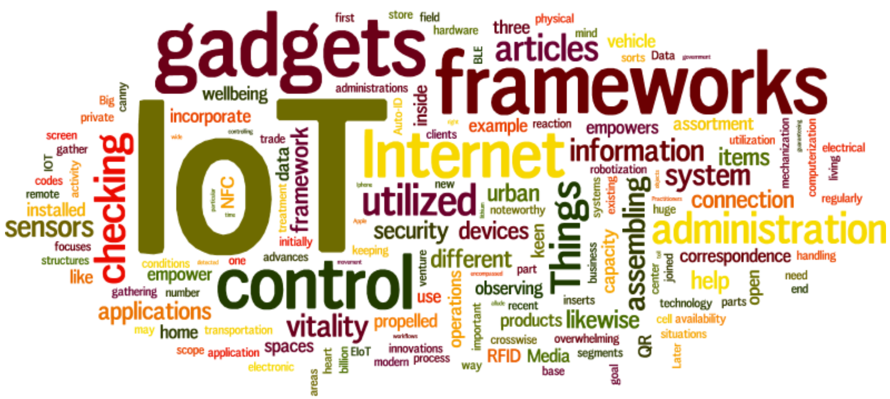
CS578: Internet of Things

IEEE 802.15.4

Standard: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6471722



Dr. Manas Khatua

Assistant Professor, Dept. of CSE, IIT Guwahati

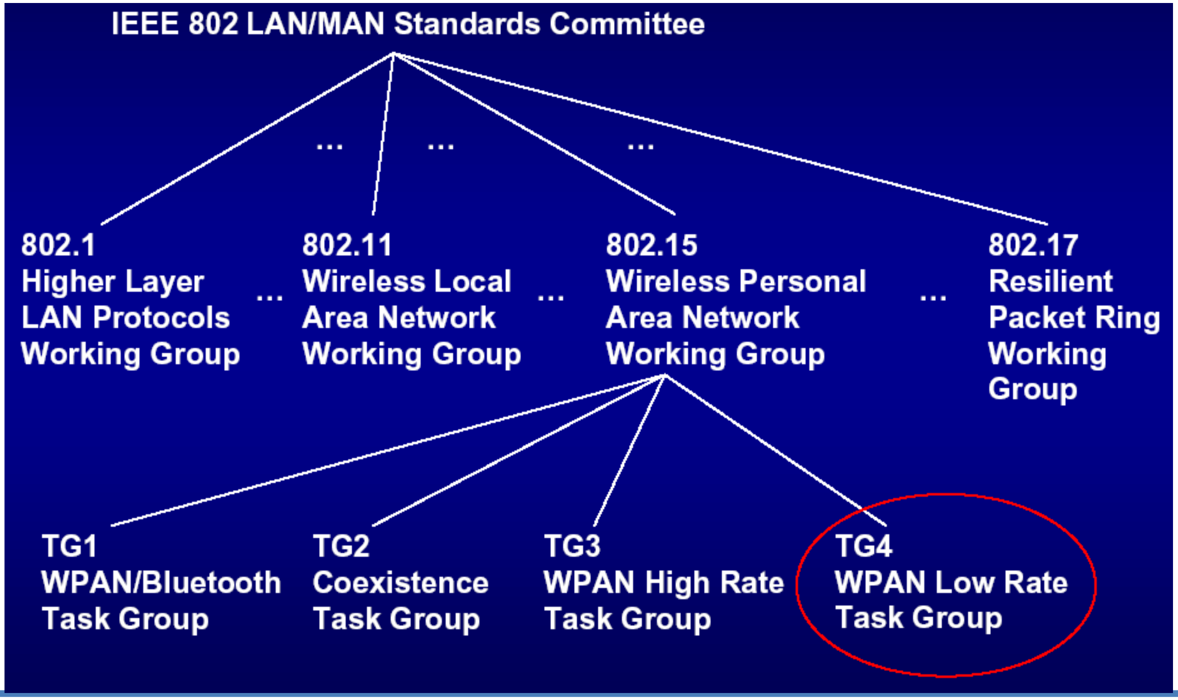
E-mail: manaskhatua@iitg.ac.in, URL: http://manaskhatua.github.io/

"The highest education makes our life in harmony with all existence." – **Rabindranath Tagore**

IEEE 802.15 Task Group 4

- TG4 defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN)

- This standard has evolved over the years:
  - IEEE 802.15.4-2003 ; IEEE 802.15.4-2006
  - IEEE 802.15.4-2011; IEEE 802.15.4-2015



- PAN
  - span a small area (e.g., a private home or an individual workspace)
  - communicate over a short distance
  - low-powered communication
  - primarily uses ad-hoc networking
  - could be wireless or wired (e.g. using USB)

IEEE 802.15.4 market feature

- Low power consumption
- Low cost system and operation
- Low offered message throughput
- Supports large network (<= 65k nodes)
- Low to no QoS guarantees
- Flexible protocol design

- IEEE 802.15.4 PHY and MAC layers **are the foundations** for several networking protocol stacks used in different market applications.
- Few well-known protocol stacks:
  - **ZigBee**
  - **ZigBee IP**
  - **6LoWPAN**
  - WirelessHART
  - Thread

- ZigBee shows how 802.15.4 can be leveraged at the PHY and MAC layers, independent of the protocol layers above.

What is ZigBee Alliance?

- An alliance of organizations with a **mission** to define
  - reliable,
  - cost effective,
  - low-power,
  - wirelessly networked,
  - monitoring and control products
  - based on an open global standard

- Alliance provides
  - interoperability,
  - certification testing, and
  - branding

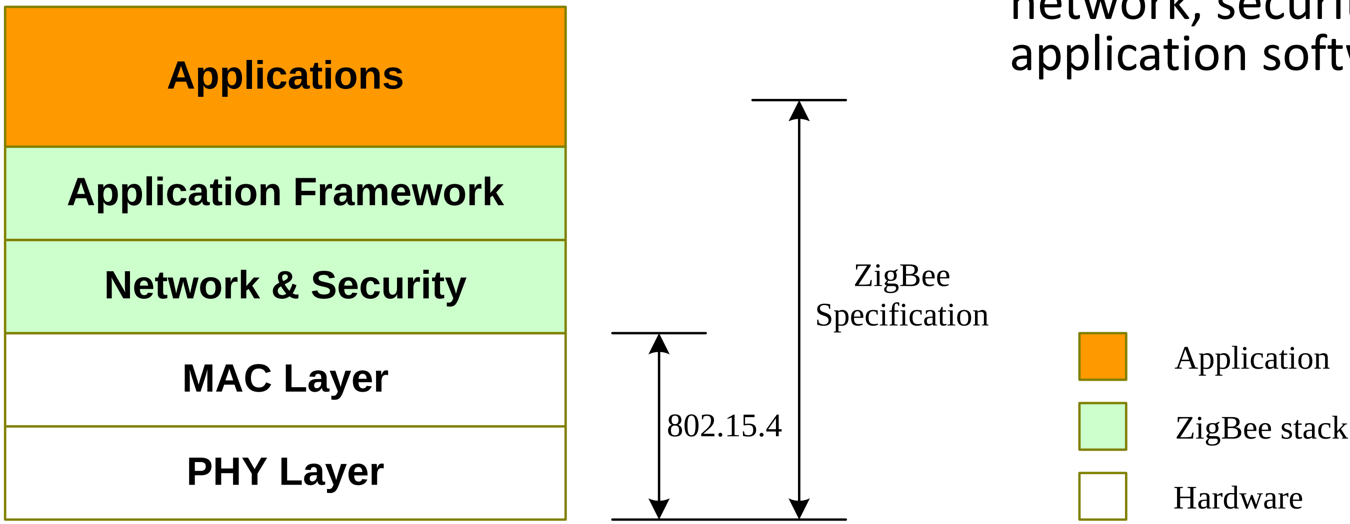
ZigBee™ Alliance

Wireless Control That Simply Works

- ZigBee Alliance
  - 45+ companies: Semiconductor mfrs, IP providers, OEMs, etc.

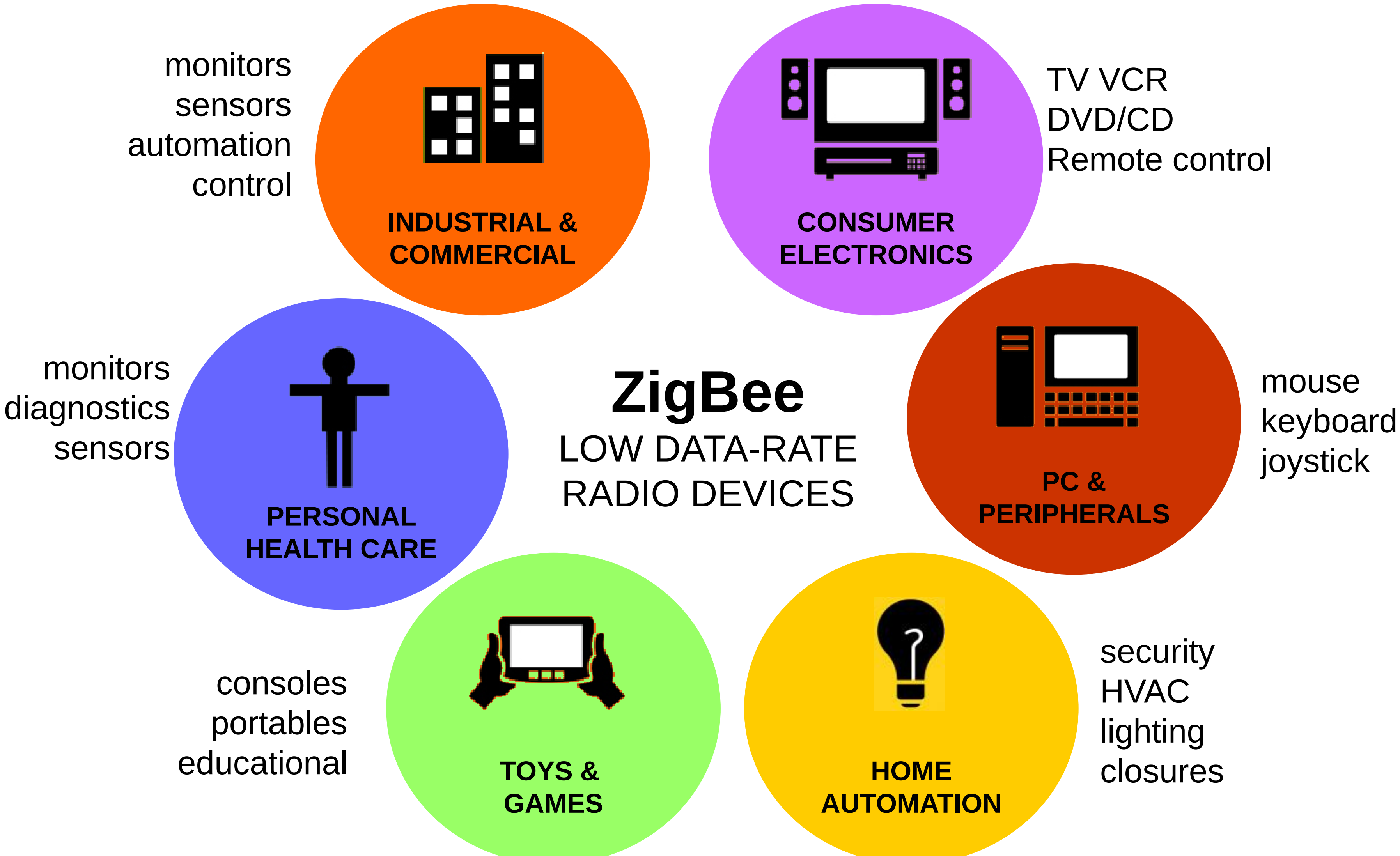
ZigBee/802.15.4 architecture

- ZigBee Alliance
  - Defining upper layers of protocol stack: from network to application, including application profiles
- IEEE 802.15.4 Working Group
  - Defining lower layers of protocol stack: MAC and PHY



- ZigBee takes full advantage of a powerful physical radio specified by IEEE 802.15.4
- ZigBee adds logical network, security and application software

ZigBee network applications



IEEE 802.15.4 PHY

IEEE 802.15.4 PHY overview

- PHY functionalities:
  - Activation and deactivation of the radio transceiver
  - Energy detection within the current channel

  - Link quality indication for received packets
  - Clear channel assessment for CSMA-CA

  - Channel frequency selection
  - Data transmission and reception

Spectrum

- Federal Communications of Commissions (FCC) in USA allocates frequency bands
- Applications using ISM (Industrial, Scientific, and Medical) band do not require a licence for stations emitting less than 1W.

FCC Band	Max. Transmit Power	Frequencies
Industrial Band	< 1 W	902 MHz – 928 M Hz
Scientific Band	< 1 W	2.4 GHz – 2.48 GHz
Medical Band	< 1 W	5.725 GHz – 5.85 GHz
U-NII (Unlicensed National Information Infrastructure)	< 40 mW	5.15 GHz – 5.25 GHz
	< 200 mW	5.25 GHz – 5.35 GHz
	< 800 mW	5.725 GHz – 5.82 GHz

- Physical layer transmission options in IEEE 802.15.4-2015
  - **2.4 GHz**, 16 channels, data rate 250 kbps
  - **915 MHz**, 10 channels, data rate 250 kbps
  - **868 MHz**, 3 channel, data rate 100 kbps

Spread Spectrum

- Idea of Spread Spectrum is to spread the information signal over a wider bandwidth to make jamming and interception more difficult.
- can be used to transmit either analog or digital data, using an analog signal
- **Types**:
  - frequency hopping spread spectrum (**FHSS**)
  - direct sequence spread spectrum (**DSSS**)

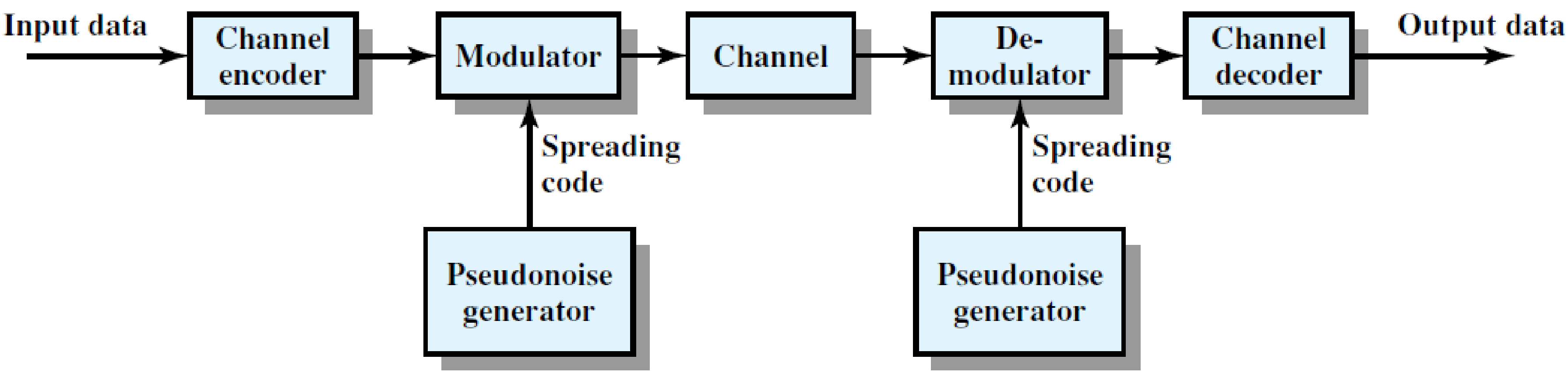


Figure 9.1 General Model of Spread Spectrum Digital Communication System

Cont…

- Pseudorandom numbers
  - generated by an algorithm using some initial value called the seed
  - produce sequences of numbers that are not statistically random, but passes reasonable tests of randomness
  - unless you know the algorithm and the seed, it is impractical to predict the sequence

- Gain from this **apparent waste of spectrum**
  - The signals gains immunity from various kinds of noise and multipath distortion.
  - Immune to jamming attack
  - It can also be used for hiding and encrypting signals.
  - Several users can independently use the same higher bandwidth with very little interference. (e.g. CDMA)

DSSS

- each bit in the original signal is represented by multiple bits in the transmitted signal, using a spreading code
- spreading code spreads the signal across a wider frequency band in direct proportion to the number of bits used

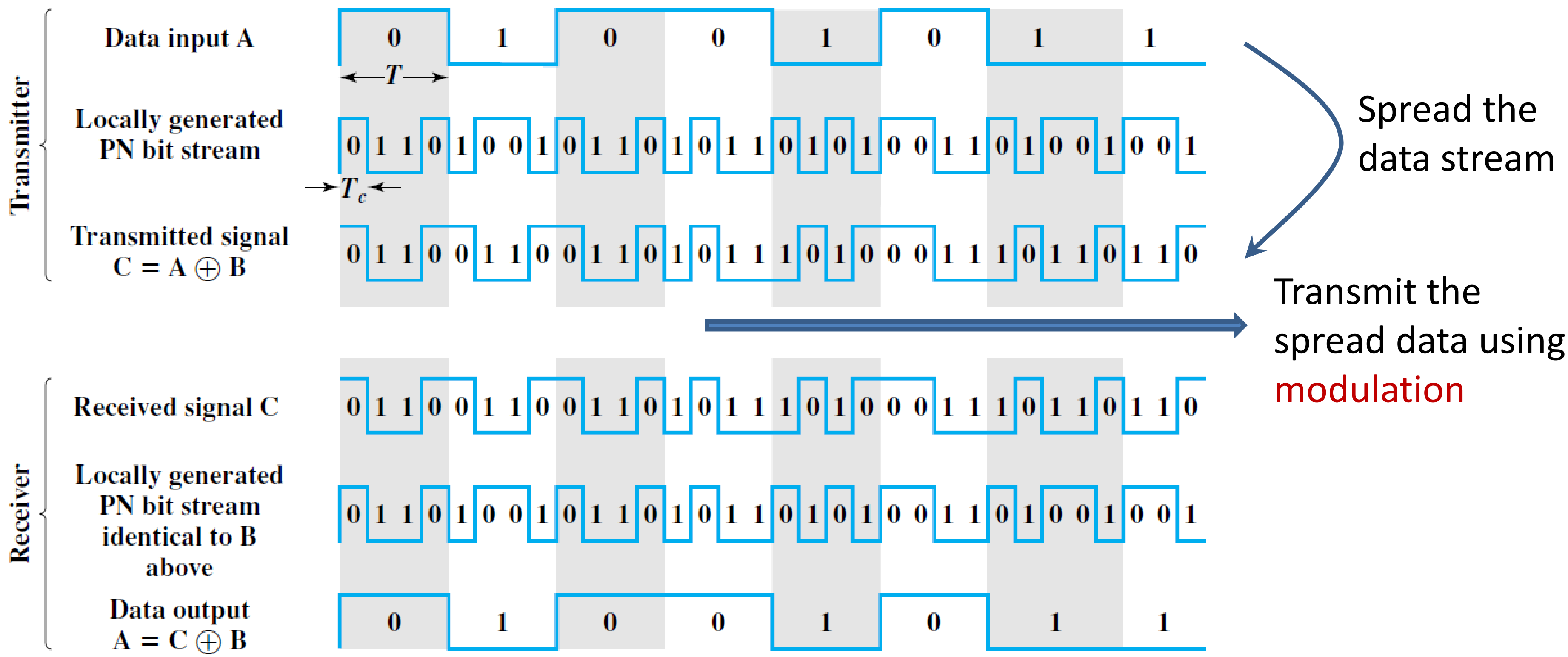


Figure 9.6 Example of Direct Sequence Spread Spectrum

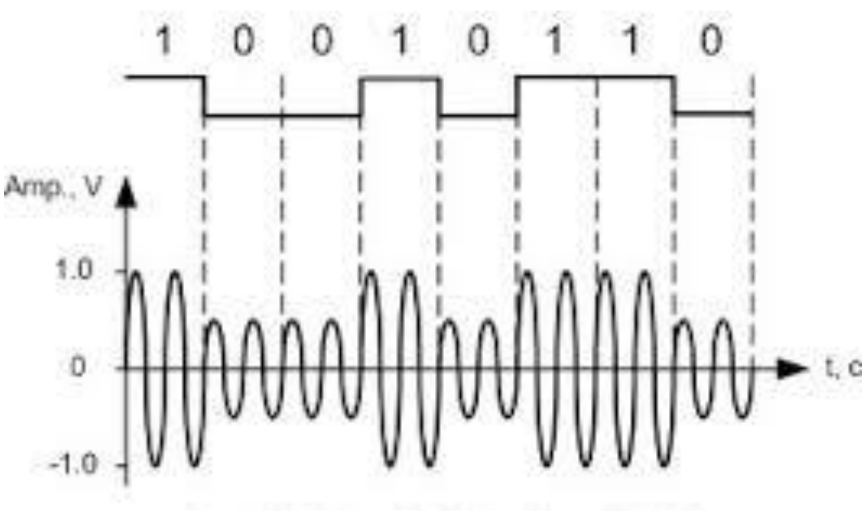
Modulation

Modulation schemes

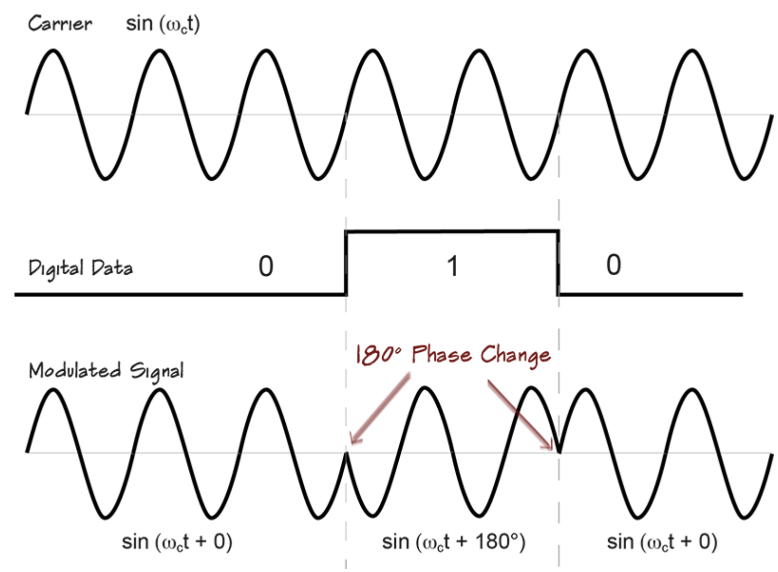
- **OQPSK PHY** : DSSS PHY employing Offset Quadrature Phase-Shift Keying (OQPSK)
- **BPSK PHY** : DSSS PHY employing binary phase-shift keying (BPSK)
- **ASK PHY** : PSSS PHY employing Amplitude Shift Keying (ASK) and BPSK

$$\textbf{ASK} \quad s(t) = \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ 0 & \text{binary } 0 \end{cases}$$

$$\textbf{BPSK} \quad s(t) = \begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t + \pi) \end{cases} = \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ -A\cos(2\pi f_c t) & \text{binary } 0 \end{cases}$$

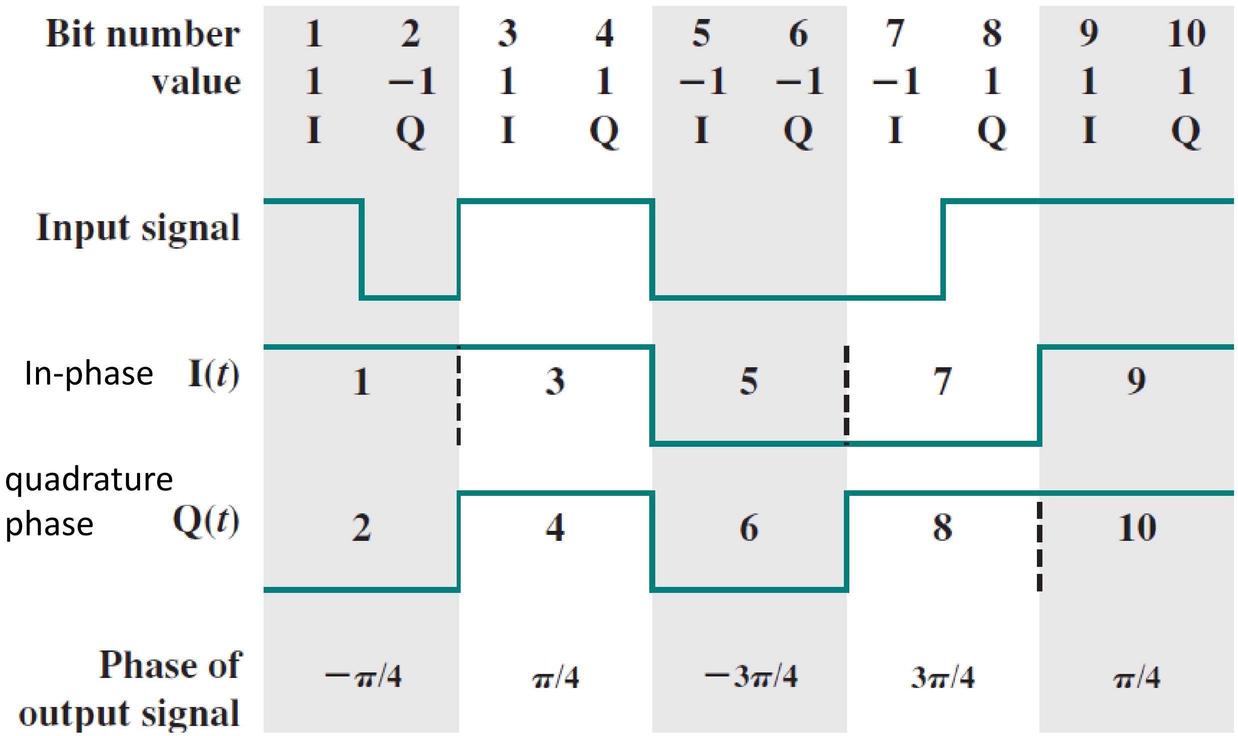


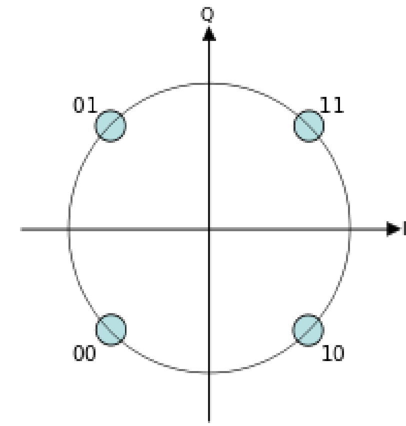
Amplitude Shift Keying (ASK)



Binary Phase-Shift Keying (BPSK)

QPSK





Constellation diagram for QPSK

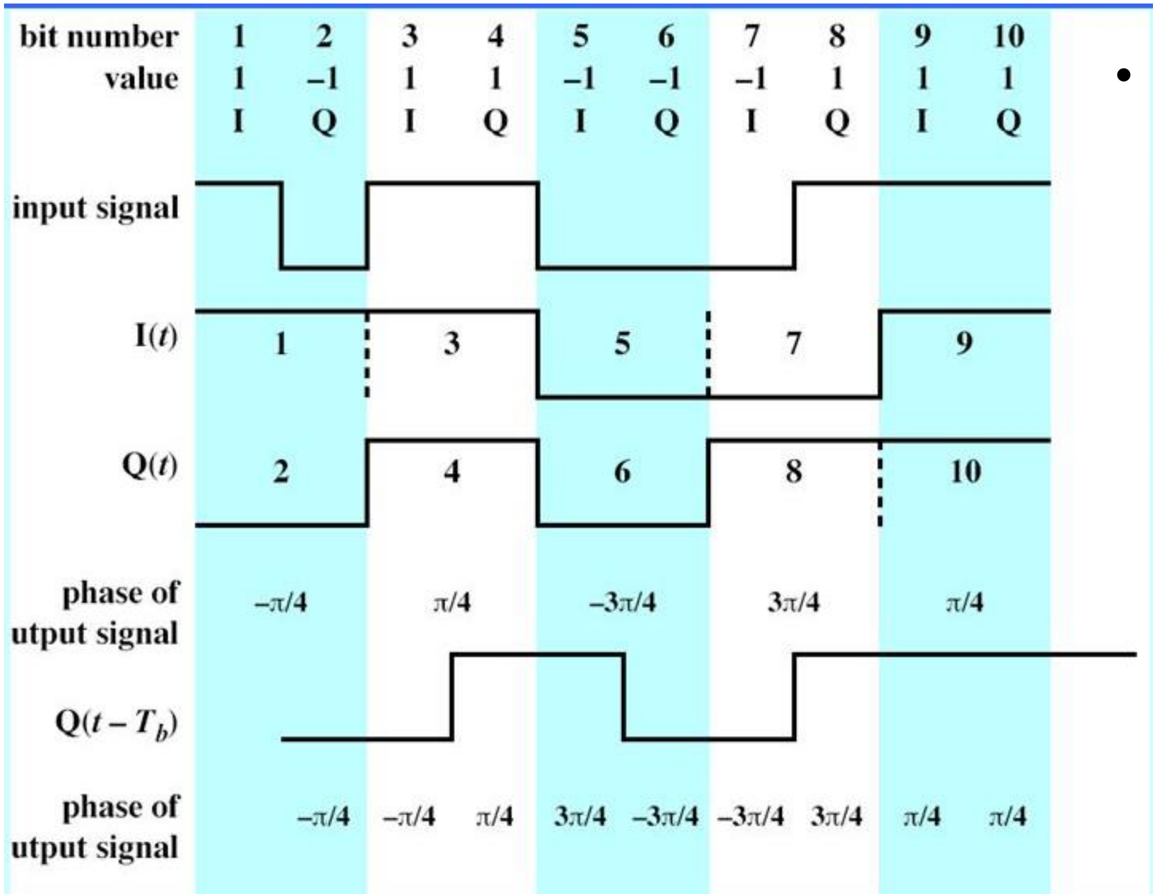
Quadrature Phase-Shift Keying (QPSK)

- More efficient use of bandwidth
  - as each signalling element represents more than one bit.

$$\textbf{QPSK} \quad s(t) = \begin{cases} A\cos\left(2\pi f_c t + \dfrac{\pi}{4}\right) & 11 \\ A\cos\left(2\pi f_c t + \dfrac{3\pi}{4}\right) & 01 \\ A\cos\left(2\pi f_c t - \dfrac{3\pi}{4}\right) & 00 \\ A\cos\left(2\pi f_c t - \dfrac{\pi}{4}\right) & 10 \end{cases}$$

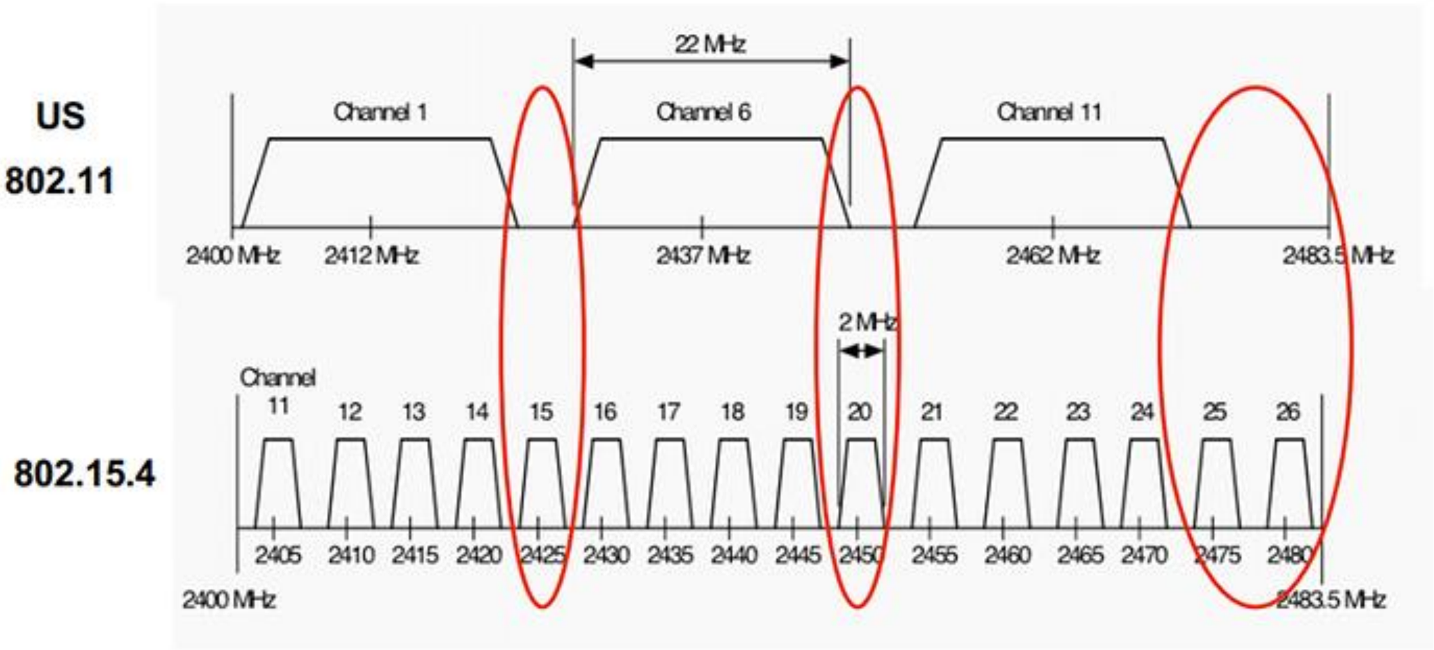
Orthogonal QPSK

- Problem in QPSK: large phase shift at high transition rate is difficult to perform. Phase shift is 180° in QPSK.



- OQPSK
  - ✓ a variation of QPSK known as offset QPSK or orthogonal QPSK
  - ✓ a delay of one bit time is introduced in the Q stream of QPSK
  - ✓ Its spectral characteristics and bit-error performance are the same as that of QPSK
  - ✓ at any time the phase change in the combined signal never exceeds 90° (π/2)

Other Attributes



- IEEE 802.15.4 does not prefer to use frequency hopping to minimize energy consumption.
- To minimize interference in 2.4 GHz band, IEEE 802.15.4 prefer channel no. 15, 20, 25, 26

- Transmission power is adjustable from 0.5 mW (min in 802.1.5.4) to 1 W (max in ISM band)
- Transmission power 1 mW provides theoretical distances as: Outdoor range 300 m; Indoor range 100 m.

Cont…

- 802.15.4 PHY provides energy detection (ED) feature
  - Application can request to asses each channel's energy level
  - Coordinator can make optimal selection of channel based on channels energy level

- 802.15.4 PHY provides link quality information (LQI) to NET and APP layers
  - Transmitter may decide to use high transmission power based on LQI
  - Applications may dynamically change 802.15.4 channels based on LQI

- 802.15.4 uses CSMA/CA which ask the PHY layer to do CCA
  - Clear Channel Assessment (CCA):
    - Can be energy threshold regardless of modulation
    - Can be detection of modulation
    - Can be both the above

PHY Frame

- PHY packet fields
  - Preamble (32 bits) – synchronization of data transmission
  - SFD (8 bits) – shall be formatted as “1110 0101”
  - PHY header (8 bits) – PSDU length
  - PSDU (0 to 127 bytes) – data field

Sync Header		PHY Header		PHY Payload
Preamble	Start of Frame Delimiter	Frame Length (7 bit)	Reserved (1 bit)	PHY Service Data Unit (PSDU)
4 Octets	1 Octets	1 Octets		0-127 Bytes

IEEE 802.15.4 MAC

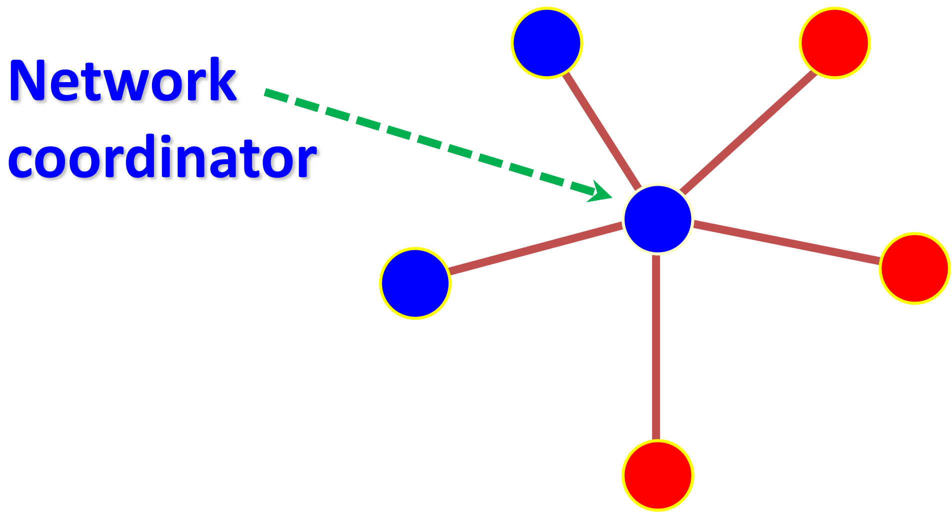
IEEE 802.15.4 Device Types

- There are two different device types :
  - full function device (**FFD**)
  - reduced function device (**RFD**)

- The **FFD** can operate in three modes by serving as
  - **PAN Coordinator**
    - scanning the network and selecting optimal RF channel
    - selecting the 16 bit PAN ID for the network
  - **Coordinator**
    - relaying messages to other FFDs including PAN coordinator
    - transmits periodic beacon (under beacon enable access mode)
    - respond to beacon requests
  - **Device**
    - cannot route messages
    - usually receivers are switched off except during transmission
    - attached to the network only as leaf nodes

- The **RFD** can only serve as:
  - **Device**

Star Topology



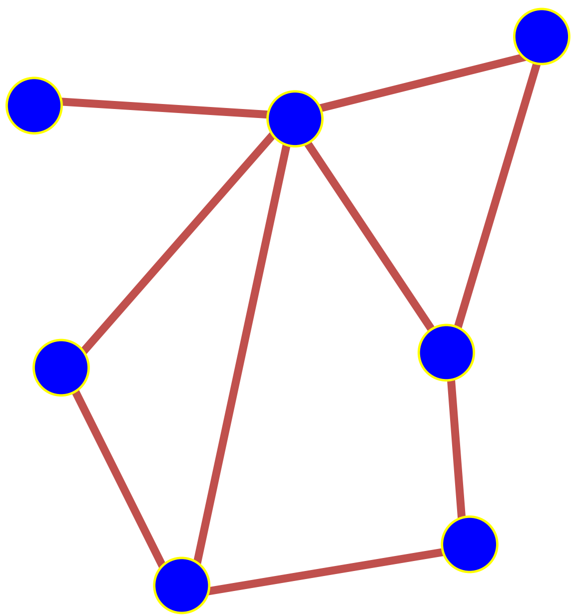
Master/slave

Full Function Device (FFD)

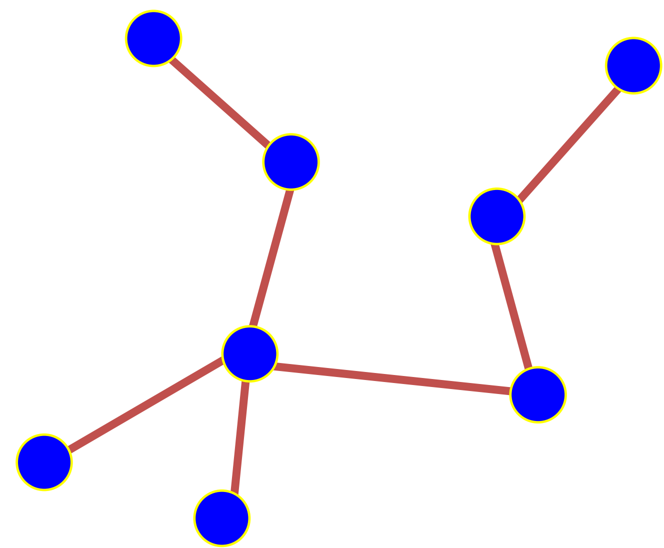
Reduced Function Device (RFD)

Communications Flow

Peer-to-Peer Topology



Point to point

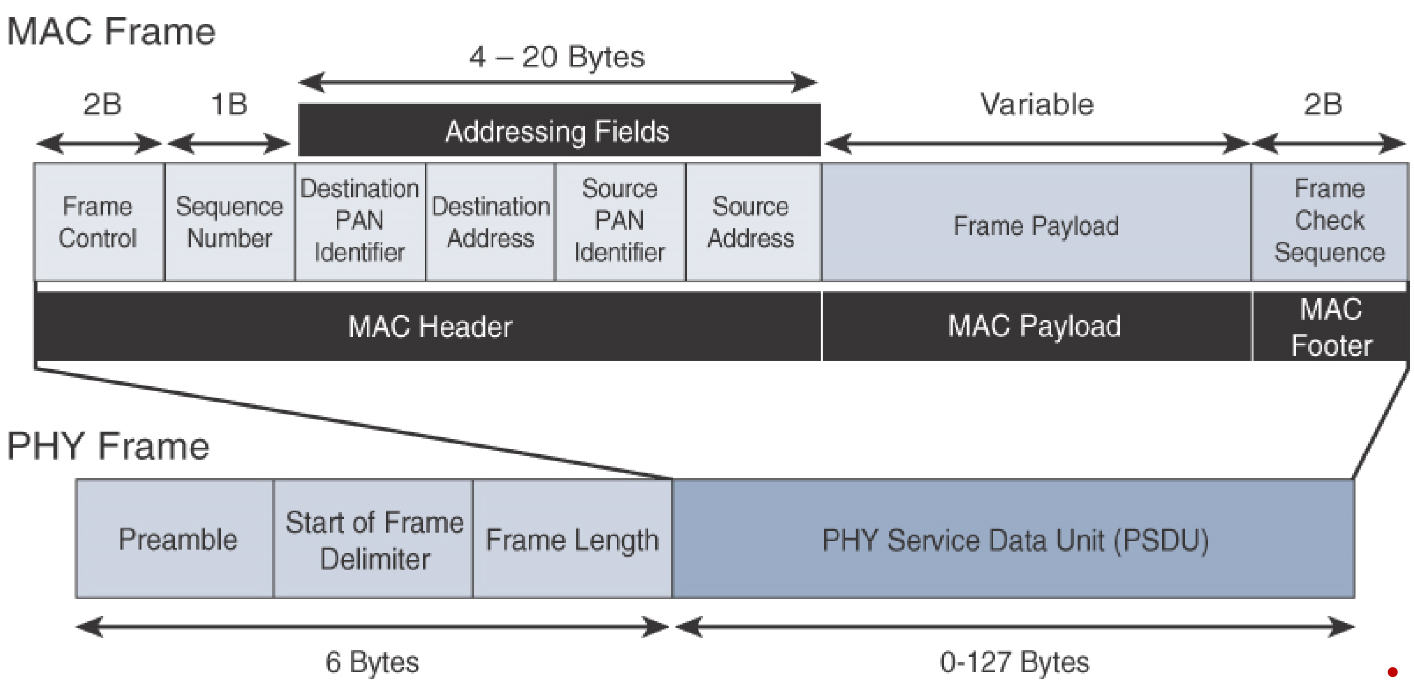


Tree

Full Function Device (FFD)

Communications Flow

General MAC Frame Format



- MAC frame types:
  - Data frame
  - ACK frame
  - Beacon frame
  - Command frame

Frame Control

Bits: 3	1	1	1	1	3	2	2	2
Frame Type	Security enabled	Frame pending	ACK required	Pan ID	**Reserved**	Dest addr mode	Frame Version	Src addr mode

Beacon Frame Format

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

Bits: 0-3	4-7	8-11	12	13	14	15
Beacon order	Superframe order	Final CAP slot	Battery life extension	Reserved	PAN coordinator	Association permit

Command Frame Format

Octets:2	1	4 to 20	1	variable	2
Frame control	Data sequence number	Address information	Command type	Command payload	Frame check sequence
MAC header			**MAC payload**		**MAC footer**

- Command Frame Types
  - Association request
  - Association response
  - Disassociation notification
  - Data request
  - PAN ID conflict notification
  - Orphan Notification
  - Beacon request
  - Coordinator realignment
  - GTS request

Data & ACK Frame Format

Data Frame

Octets:2	1	4 to 20	variable	2
Frame control	Data sequence number	Address information	Data payload	Frame check sequence
MAC header			**MAC Payload**	**MAC footer**

ACK Frame

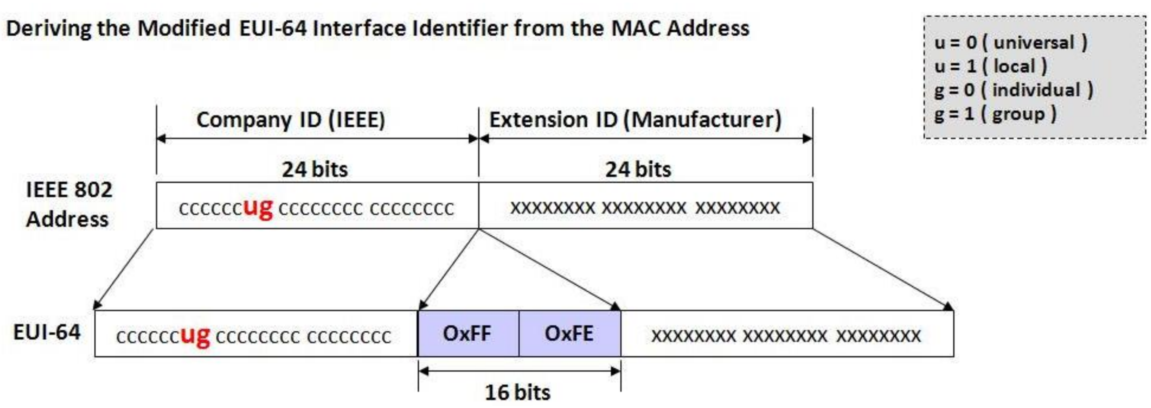
Octets:2	1	2
Frame control	Data sequence number	Frame check sequence
MAC header		**MAC footer**

Device Addressing

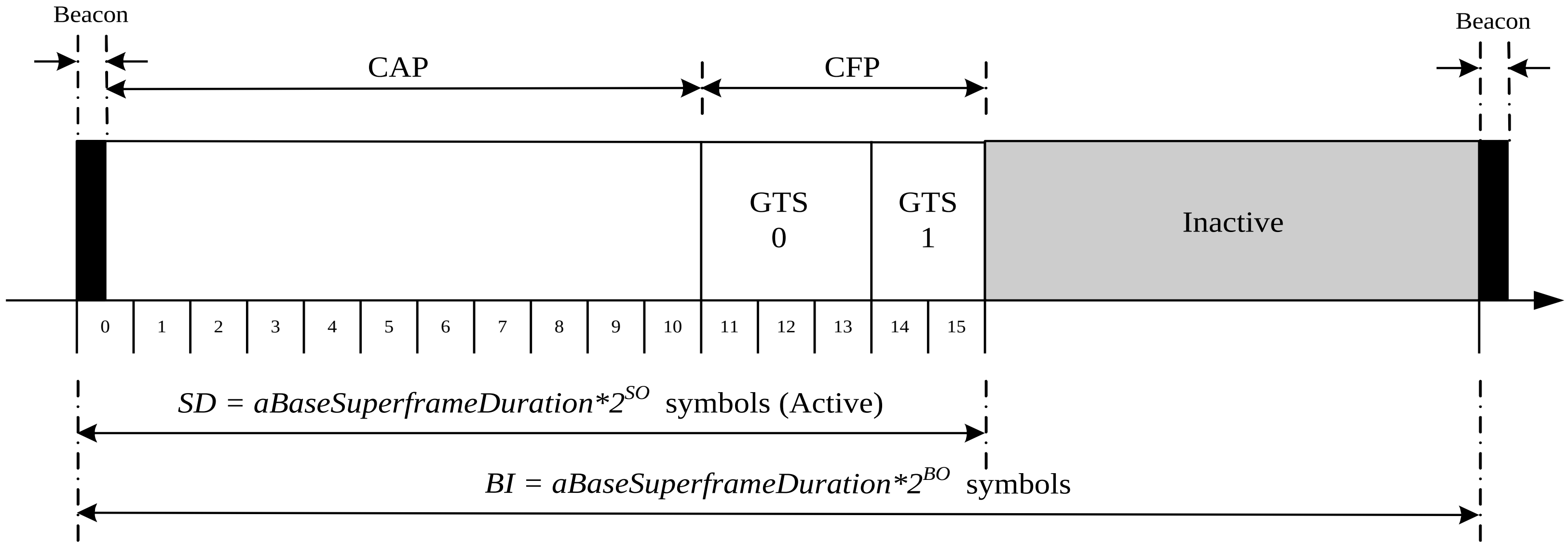
- Two or more devices communicating on the same physical channel constitute a WPAN.
  - A WPAN includes at least one FFD (PAN coordinator)
  - Each independent PAN will select a unique PAN identifier

- Each device operating on a network has a unique 64-bit address, called extended unique identifier (EUI-64)
  - This address can be used for direct communication in the PAN

- A device also has a 16-bit short address, which is allocated by the PAN coordinator when the device associates with its coordinator.



Superframe



- A superframe is divided into two parts
  - Inactive: all station sleep.
    - no communication
    - nodes can turn their radios off and go into power saving mode
  - Active:
    - Active period is divided into 16 slots
    - 16 slots are further divided into two parts
      - Contention access period (**CAP**)
      - Contention free period (**CFP**)
      - Beacon only period (**BOP**)

- superframe order (SO) : decides the length of the active portion in a superframe
- beacon order (BO) : decides the length of a superframe or beacon transmission period
- beacon-enabled network should satisfy $0 \leqq SO \leqq BO \leqq 14$
- PAN coordinator decides SO, BO

Cont…

- *aBaseSlotDuration* = The number of symbols forming a superframe slot when *the superframe order (SO)* is equal to zero = 60 PHY symbols

- *aBaseSuperframeDuration* = The number of symbols forming a superframe when *the superframe order (SO)* is equal to zero. = *aBaseSlotDuration* × aNumSuperframeSlots

- *aNumSuperframeSlots* = The number of slots contained in any superframe = 16

- Length of a superframe can range from 15.36 *msec* to 215.7 *sec* (= 3.5 min).

- Beacons are used for
  - starting superframes
  - synchronizing with other devices
  - announcing the existence of a PAN
  - informing pending data in coordinators

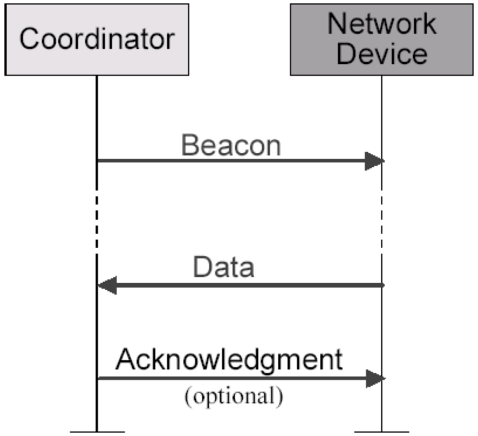
Cont…

- In a “beacon-enabled” network (**i.e. uses superframe structure**)
  - Devices use the slotted CAMA/CA mechanism to contend for the channels
  - FFDs which require fixed rates of transmissions can ask for *guarantee time slots (GTS)* from the coordinator
- In a “nonbeacon-enabled” network (**i.e. do not use ssuperframe structure**)
  - Devices use the unslotted CAMA/CA mechanism for channel access
  - GTS shall not be permitted
- CSMA/CA is not used for Beacon transmission; and Data frame transmission during CFP
- Each device will be
  - **active for** $2^{-(BO-SO)}$ portion of the time
  - **sleep for** $1 - 2^{-(BO-SO)}$ portion of the time
- Duty Cycle:

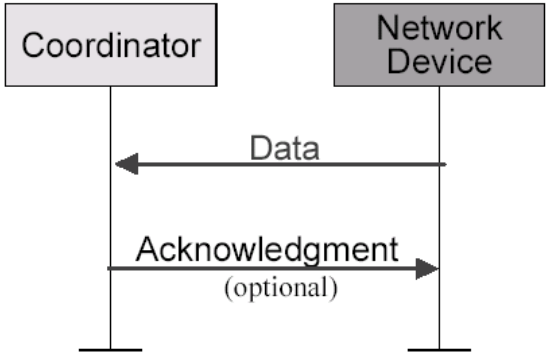
BO-SO	0	1	2	3	4	5	6	7	8	9	≧10
Duty cycle (%)	100	50	25	12	6.25	3.125	1.56	0.78	0.39	0.195	< 0.1

Data Transfer Model (I)

- Data transferred **from** device **to** coordinator
  - In a beacon-enable network,
    - a device finds the beacon to synchronize to the superframe structure.
    - Then it uses **slotted CSMA/CA** to transmit its data.
  - In a non-beacon-enable network,
    - device simply transmits its data using **unslotted CSMA/CA**



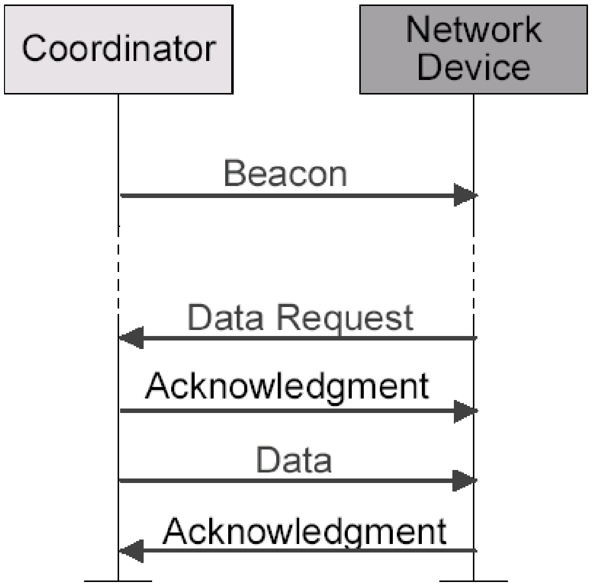
Communication to a coordinator
In a beacon-enabled network

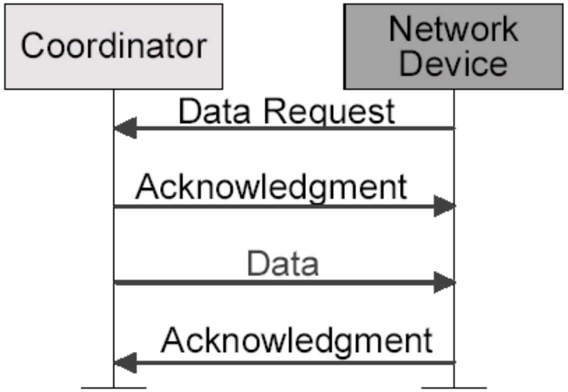


Communication to a coordinator
In a non-beacon-enabled network

Data Transfer Model (II)

- Data transferred **from** coordinator **to** device
  - in a beacon-enabled network:
    - The coordinator indicates in the beacon that some data is pending.
    - A device periodically listens to the beacon and transmits a Data Request command using slotted CSMA/CA.
    - Then ACK, Data, and ACK follow …





- Data transferred **from** coordinator **to** device
  - in a non-beacon-enable network:
    - The device transmits a Data Request using unslotted CSMA/CA.
    - If the coordinator has its pending data, an ACK is replied.
    - Then the coordinator transmits Data using unslotted CSMA/CA.
    - If there is no pending data, a data frame with zero length payload is transmitted.

Channel Access Mechanism

- CSMA/CA random channel access is used more often
  - ➢ beacon-enabled networks → slotted CSMA/CA channel access mechanism

    In slotted CSMA/CA:

    - The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator
    - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
    - The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period
  - ➢ nonbeacon-enabled networks → unslotted CSMA/CA channel access mechanism

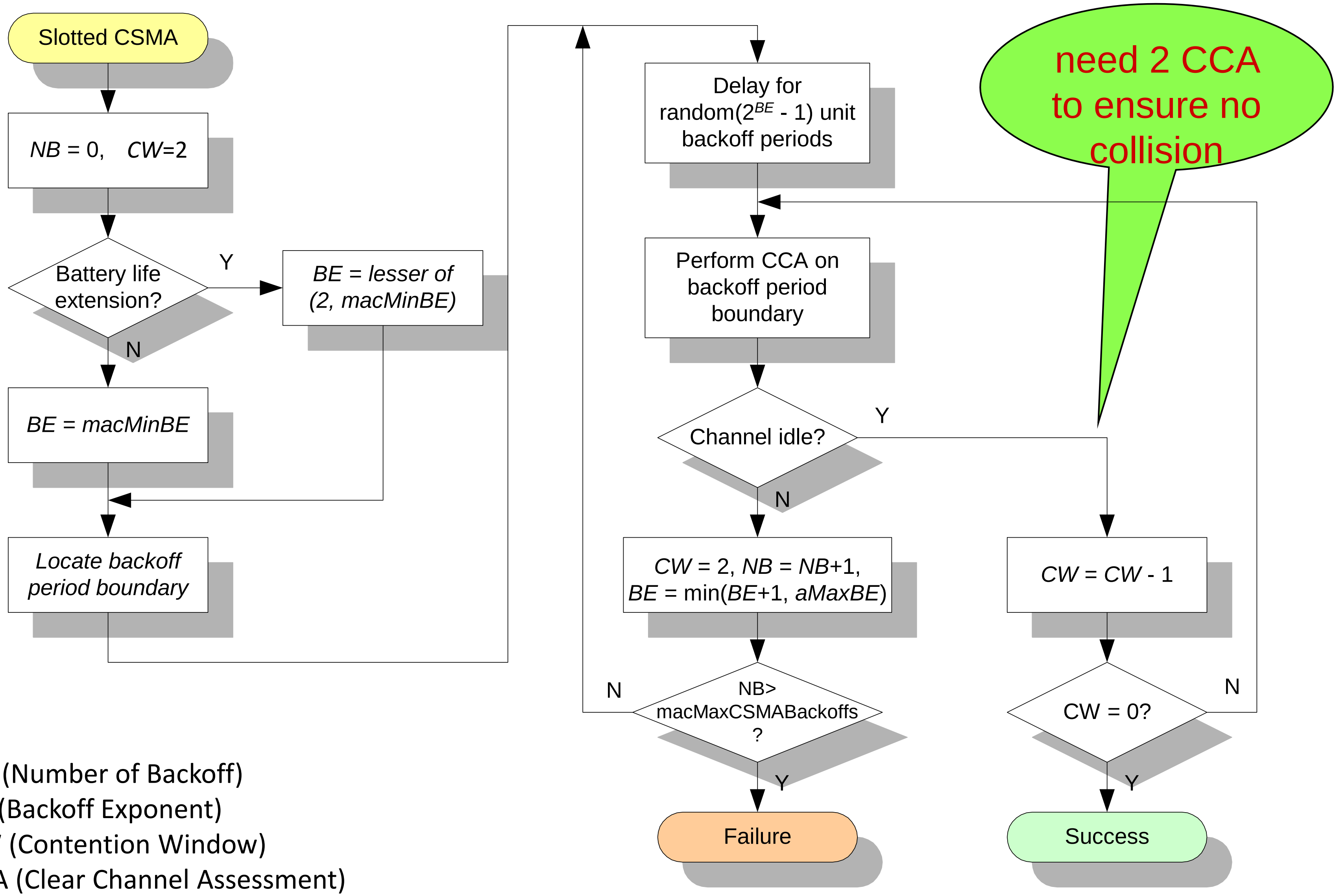
    In unslotted CSMA/CA:

    - The backoff periods of one device are not related in time to the backoff periods of any other device in the PAN.
- Algorithms runs using units of time called backoff periods, where one backoff period shall be equal to *aUnitBackoffPeriod*.

Slotted CSMA/CA algorithm

- Each device maintains 3 variables for each transmission attempt
  - NB (Number of Backoff): number of times that backoff has been taken in this attempt
    - if exceeding macMaxCSMABackoff, the attempt fails
  - BE (Backoff Exponent): the backoff exponent is related to how many backoff periods a device shall wait before attempting to assess a channel.
    - the number of backoff periods is greater than the remaining number of backoff periods in the CAP
      - MAC sublayer shall pause the backoff countdown at the end of the CAP,
      - and resume it at the start of the CAP in the next superframe
  - CW (Contention Window): contention window length, the number of clear slots that must be seen after each backoff
    - always set to 2 and count down to 0 if the channel is sensed to be clear
    - The design is for some PHY parameters, which require 2 CCA for efficient channel usage.
- Battery Life Extension (BLE):
  - designed for very low-power operation, where a node only contends in the first few slots

Cont...

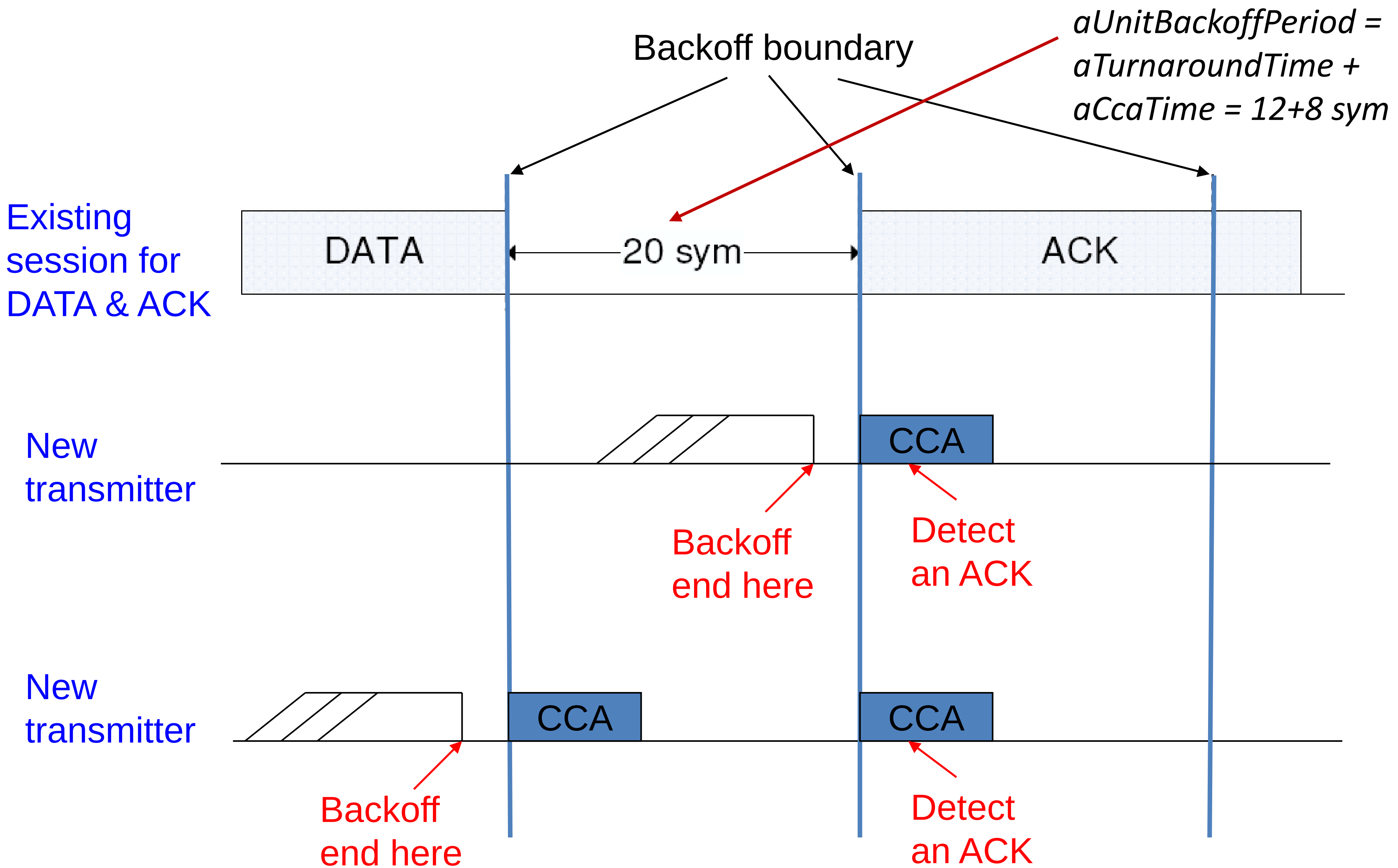


NB (Number of Backoff)
BE (Backoff Exponent)
CW (Contention Window)
CCA (Clear Channel Assessment)

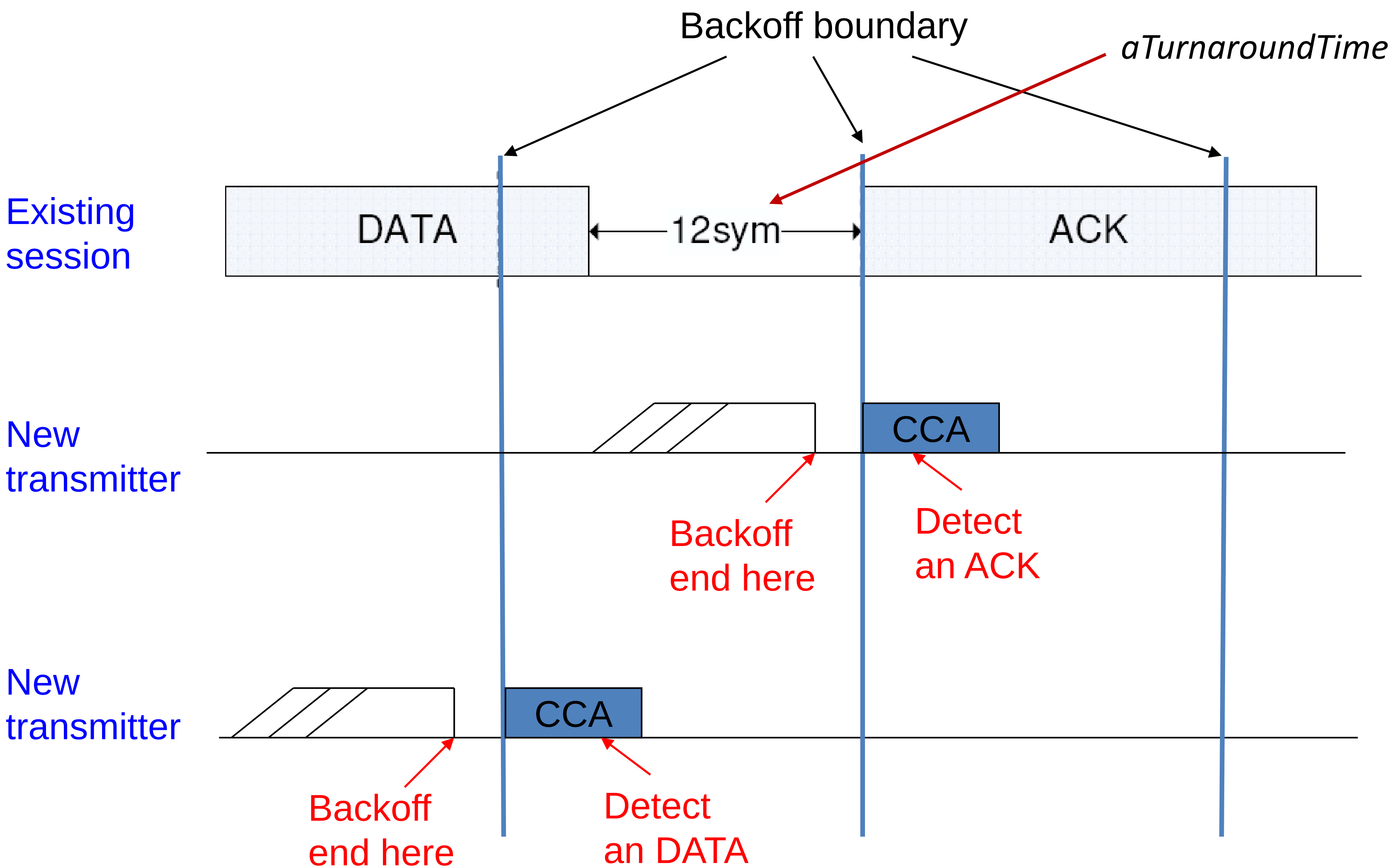
Why 2 CCAs to Ensure Collision-Free

- Each CCA occurs at the boundary of a backoff slot (= 20 PHY symbols), and each CCA time = 8 PHY symbols.
- The standard species that a transmitter node performs the CCA twice in order to protect acknowledgment (ACK).
  - When an ACK packet is expected, the receiver shall send it after a t_{ACK} time on the backoff boundary
    - t_{ACK} varies from 12 to 31 symbols
  - One-time CCA of a transmitter may potentially cause a collision between a newly-transmitted packet and an ACK packet.
  - (See examples below)

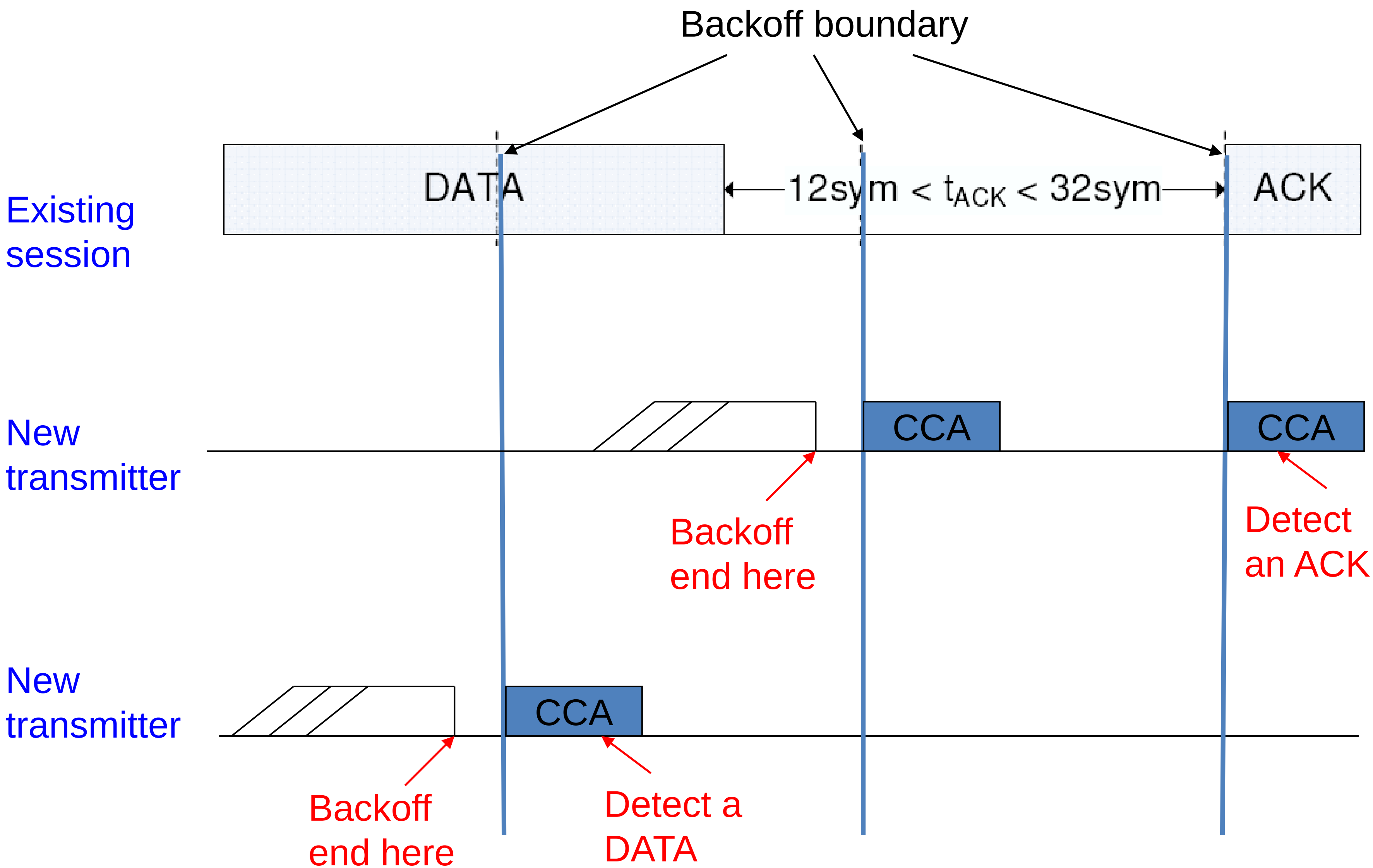
Why 2 CCAs (case 1)



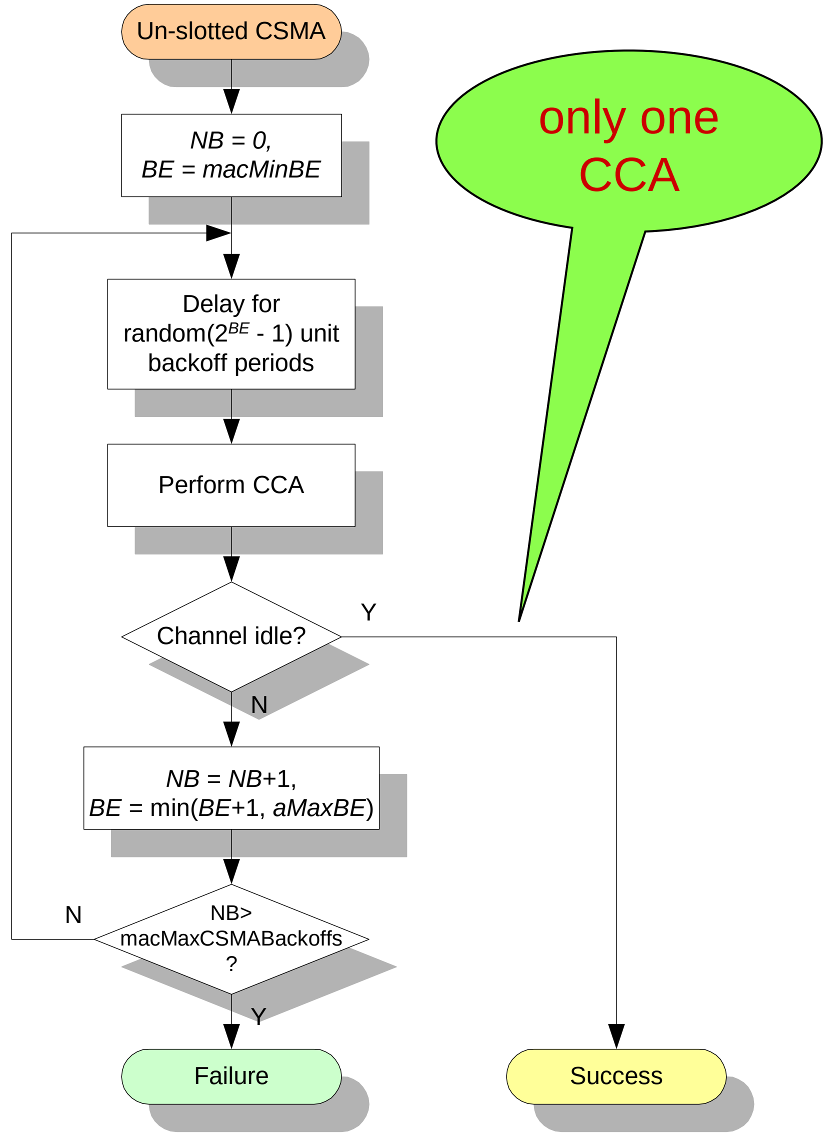
Why 2 CCAs (Case 2)



Why 2 CCAs (Case 3)



Unslotted CSMA/CA



NB (Number of Backoff)
BE (Backoff Exponent)
CW (Contention Window)
CCA (Clear Channel Assessment)

GTS Concepts

- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe
- A GTS shall only be allocated by the PAN coordinator
- The PAN coordinator can allocated up to 7 GTSs at the same time
- The PAN coordinator decides whether to allocate GTS based on:
  - Requirements of the GTS request
  - The current available capacity in the superframe
- A GTS can be deallocated
  - At any time at the discretion of the PAN coordinator or
  - By the device that originally requested the GTS
- A device that has been allocated a GTS may also operate in the CAP
- A data frame transmitted in an allocated GTS shall use only short addressing

Cont…

- Before GTS starts, the GTS direction shall be specified as either transmit or receive
  - Each device may request one transmit GTS and/or one receive GTS

- A device shall only attempt to allocate and use a GTS if it is currently tracking the beacon

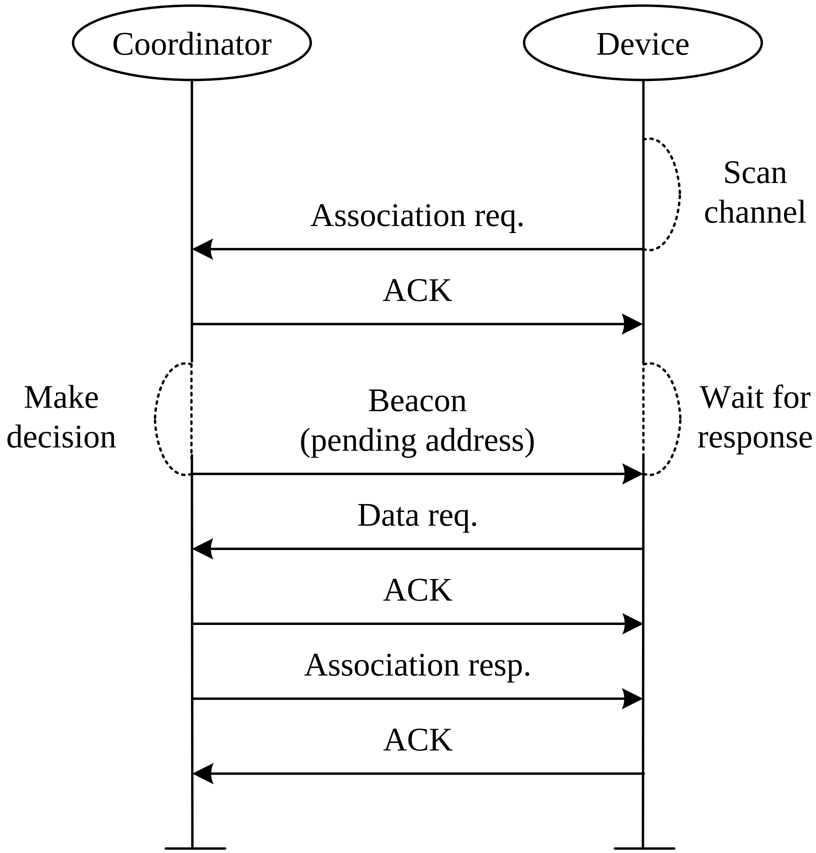
- If a device loses synchronization with the PAN coordinator, all its GTS allocations shall be lost

- The use of GTSs by an RFD is optional

Association Procedures

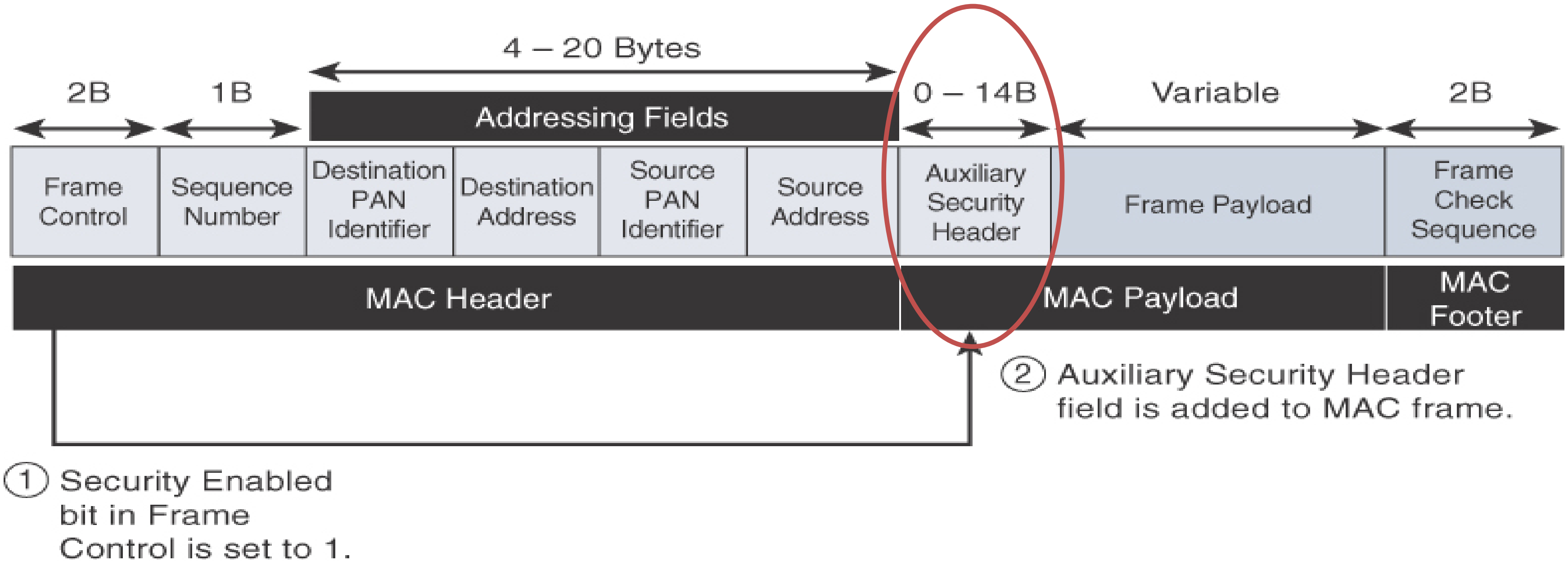
- A device becomes a member of a PAN by associating with its coordinator

- **Procedures**:



- The ACK to an Association Request command does not mean that the device has associated.
- In IEEE 802.15.4, association results are announced in an indirect fashion.
  - A coordinator responds to Association Requests by appending devices' long addresses in Beacon frames
- Devices need to send a data request to the coordinator to acquire the association result
- After associating to a coordinator, a device will be assigned a 16-bit *short address*.

Security



- IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm

- Message integrity code (MIC), which is calculated for the entire frame using the same AES key, to validate the data that is sent

Limitations in 802.15.4

- **Disadvantages of IEEE 802.1.5.4**
  - MAC reliability
  - unbounded latency
  - multipath fading

- **IEEE 802.15.4e** amendment of 802.15.4-2011 expands the MAC layer feature set
  - to remedy the disadvantages of 802.15.4.
  - to better suitable in factory and process automation, and smart grid
  - Main modifications were:
    - frame format,
    - security,
    - determinism mechanism, and
    - frequency hopping

- **IEEE 802.15.4g** amendment of 802.15.4-2011 expands mainly PHY layer feature set
  - to optimize large outdoor wireless mesh networks for field area networks (FANs)
  - to better suitable in smart grid or smart utility network (SUN) communication
  - Main modifications were:
    - New PHY definitions
    - some MAC modifications needed to support the new PHY

Thanks!

Figures and slide materials are taken from the following sources:

1. David Hanes *et al.*, “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, 1st Edition, 2018, Pearson India.
2. Oliver Hersent et al., “The Internet of Things: Key Applications and Protocols”, 2018, Wiley India Pvt. Ltd.