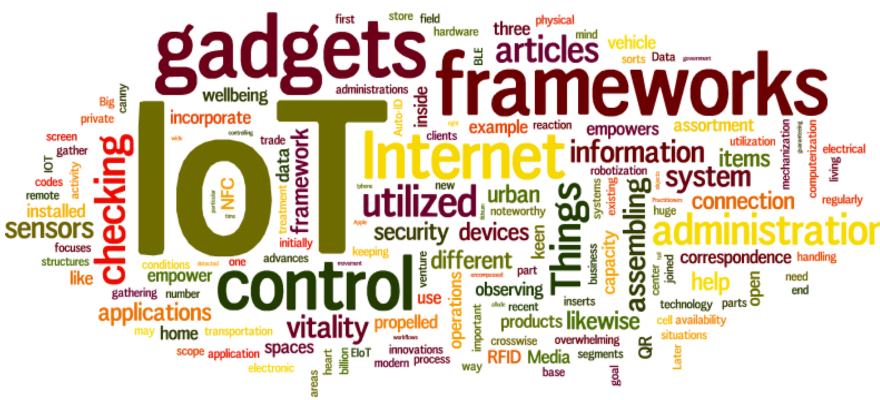
CS578: Internet of Things

IEEE 802.15.4

Low-Rate Wireless Networks

2011 version: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6012487
2015 version: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7460875
2020 version: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9144691



Dr. Manas Khatua
Assistant Professor, Dept. of CSE, IIT Guwahati
E-mail: manaskhatua@iitg.ac.in

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

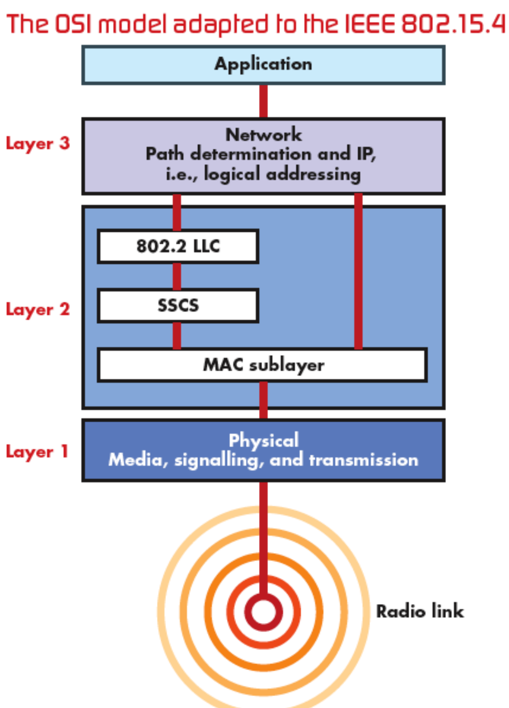
IEEE 802.15.4 LR-WPAN

- A low-rate wireless personal area network (LR-WPAN) is a
  - ✓ simple,
  - ✓ low-cost communication network
  - ✓ that allows wireless connectivity in applications
  - ✓ with limited power and
  - ✓ relaxed throughput requirements.

- The **main objectives** of an LR-WPAN are
  - ✓ ease of installation,
  - ✓ reliable data transfer,
  - ✓ extremely low cost,
  - ✓ a reasonable battery life,
    - ✓ while maintaining a simple and flexible protocol.

Reference: IEEE Std 802.15.4™-2020, "IEEE Standard for **Low-Rate Wireless Networks**",
Developed by the LAN/MAN Standards Committee of the IEEE Computer Society, Approved on 6 May 2020.

IEEE 802.15.4 Stack – PHY & MAC



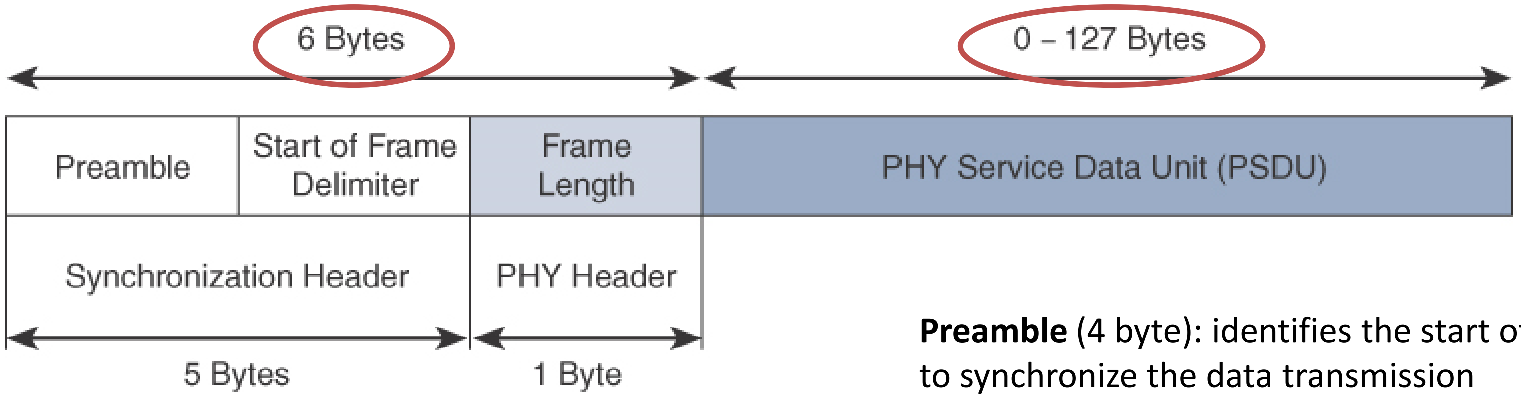
LLC: Logical Link Control – provides protocol multiplexing
SSCS: Service Specific Convergence Sublayer

- IEEE 802.15.4 standard is limited to the **PHY & MAC** Layers
- IEEE 802.15.4 standard PHY provides the PHY data service and PHY management services:
  - The **PHY data service** enables the transmission and reception of PHY protocol data units (PPDU) across the physical radio channel.
  - The **PHY's features** include
    - radio transceiver activation/deactivation,
    - radio channel selection,
    - energy level detection (ED) ,
    - received signal quality (RSI) or link quality indicator (LQI),
    - clear channel assessment (CCA),
    - channel selection
    - transmitting and receiving packets in 2.4-GHz band.
- IEEE 802.15.4 standard MAC provides the MAC data service and MAC management services.
  - The **MAC data service** enables transmission of MAC protocol data units (MPDU) across the PHY data service.
  - The **MAC sublayer features** include
    - beacon management,
    - channel access,
    - GTS management,
    - frame validation,
    - ACK frame delivery, and
    - association and disassociation.

Image Source: https://www.embedded.com/ieee-802-15-4-zigbee-hardware-and-software-open-the-applications-window/

IEEE 802.15.4 PHY

IEEE 802.15.4 PHY Layer



IEEE 802.15.4 PHY Frame Format

Preamble (4 byte): identifies the start of the frame; used to synchronize the data transmission

SFD (1 byte): informs the receiver about the starting point of frame content. It shall be formatted as “1110 0101”

PHY functionalities:

- Activation & deactivation of the radio transceiver
- Energy level detection (ED) within the current channel

- Link quality indication (LQI) or received signal quality (RSI) for received packets
- Clear channel assessment (CCA) for CSMA-CA

- Channel frequency selection
- Data packet transmission and reception at given frequency

Spectrum

- Federal Communications of Commissions (FCC) in USA decides frequency bands
- Applications using ISM 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

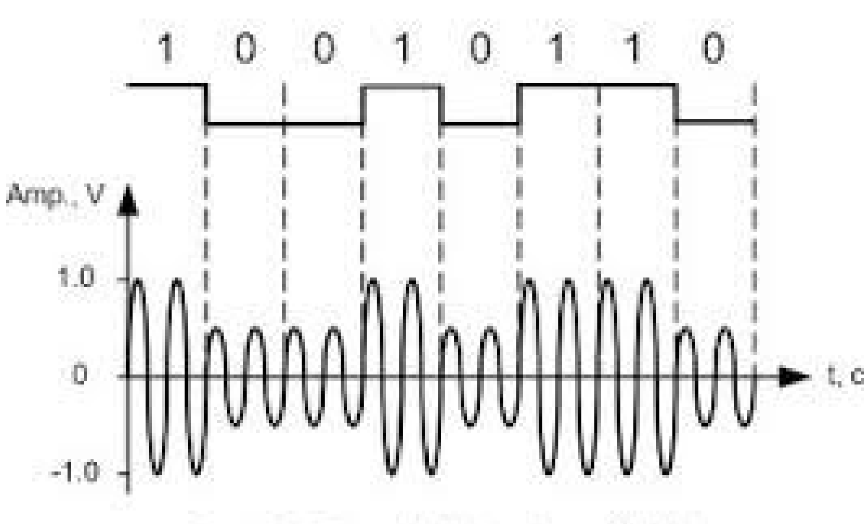
- Physical layer transmission options in IEEE 802.15.4-2015
  - **2.4 GHz**, 16 channels, data rate 250 kbps
  - **915 MHz**, 10 channels, data rate 250 kbps
  - **868 MHz**, 3 channel, data rate 100 kbps

Modulation

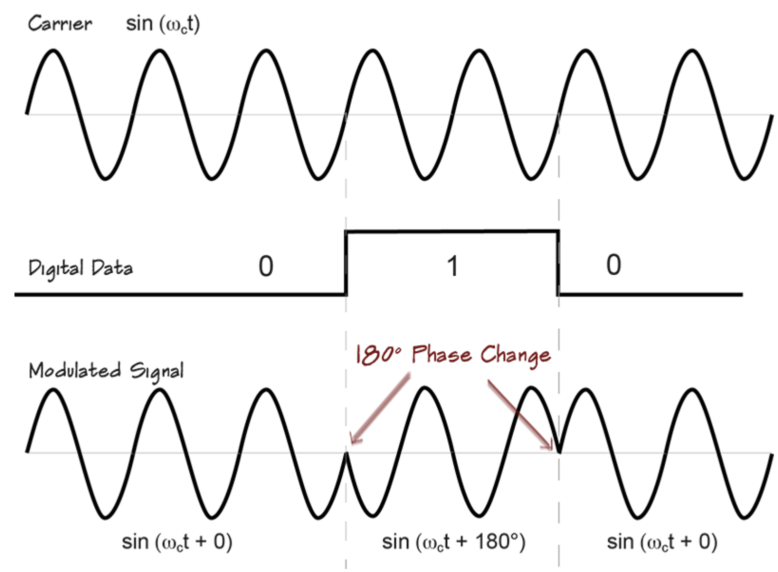
Modulation is the process by which some characteristic of a carrier wave is varied in accordance with an information/ modulating signal.

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

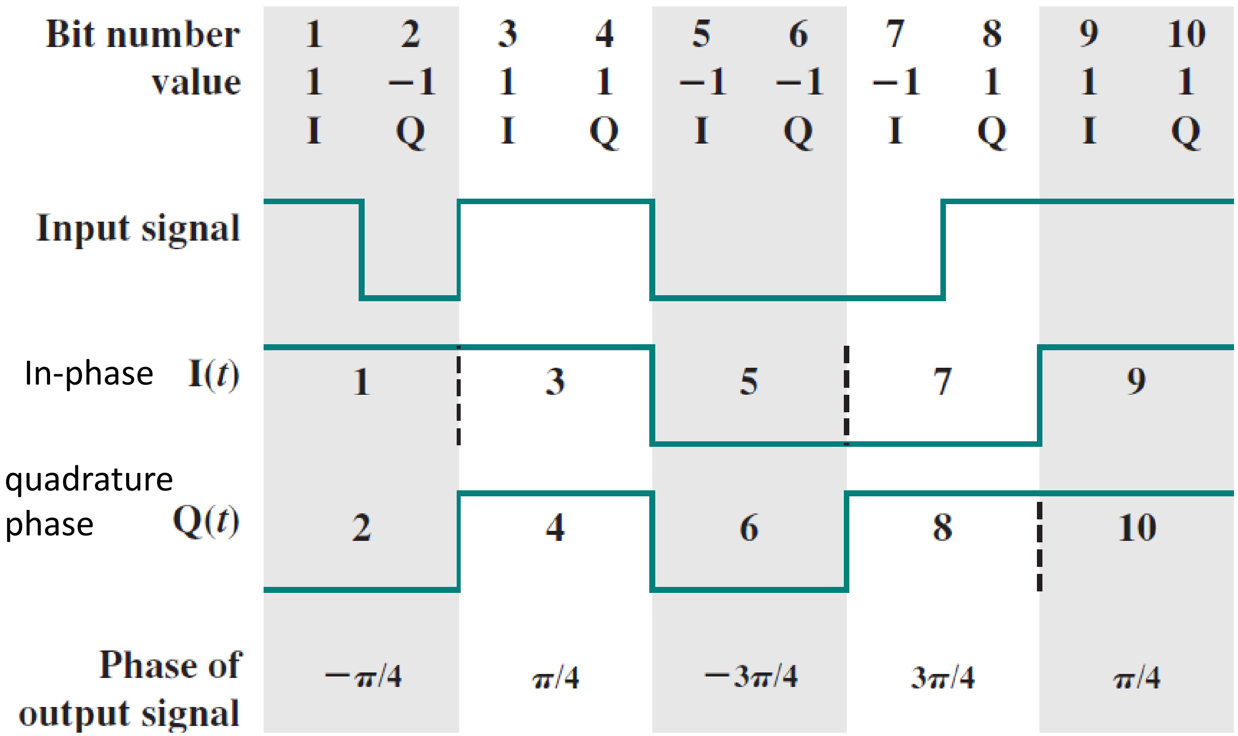


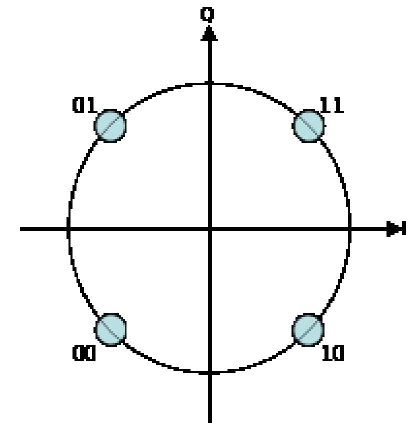
Amplitude Shift Keying (ASK)



Binary Phase-Shift Keying (BPSK)

QPSK





Constellation diagram for QPSK

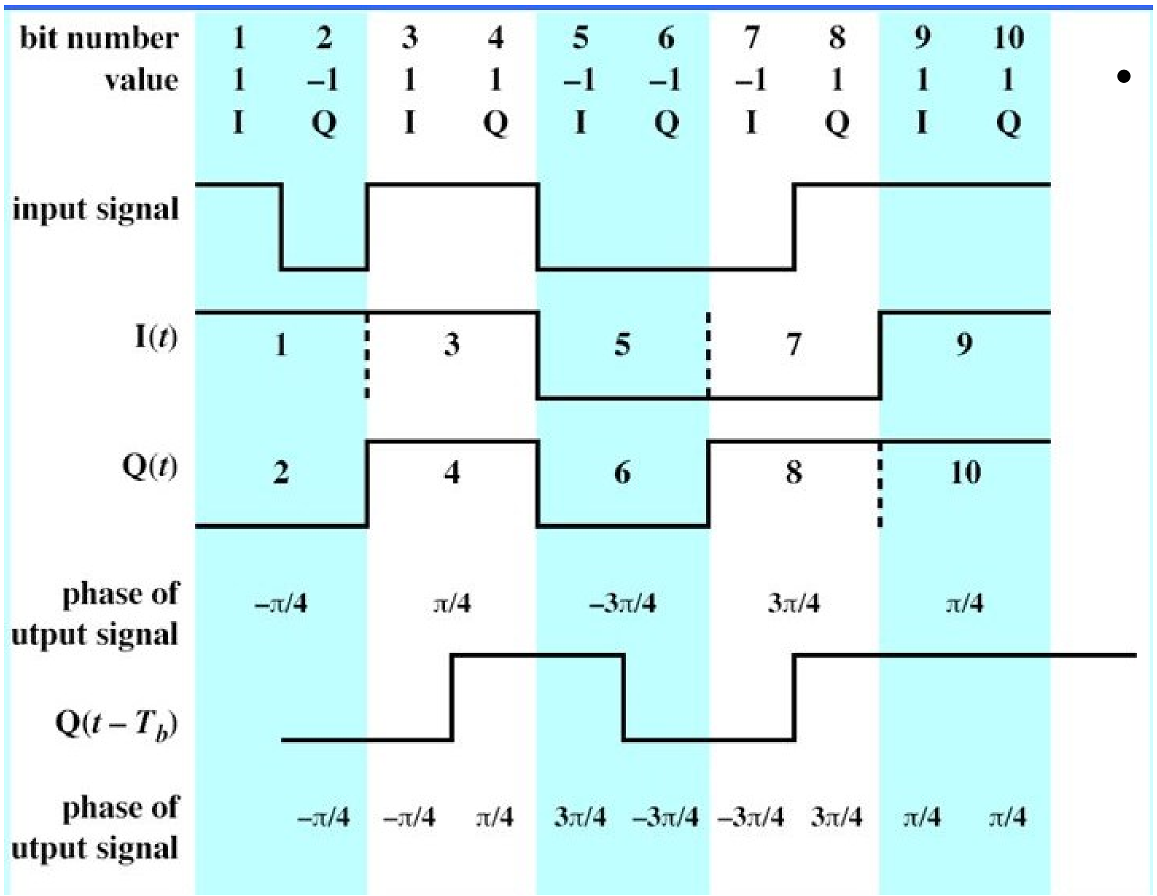
Quadrature Phase-Shift Keying (QPSK)

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

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

Orthogonal QPSK

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

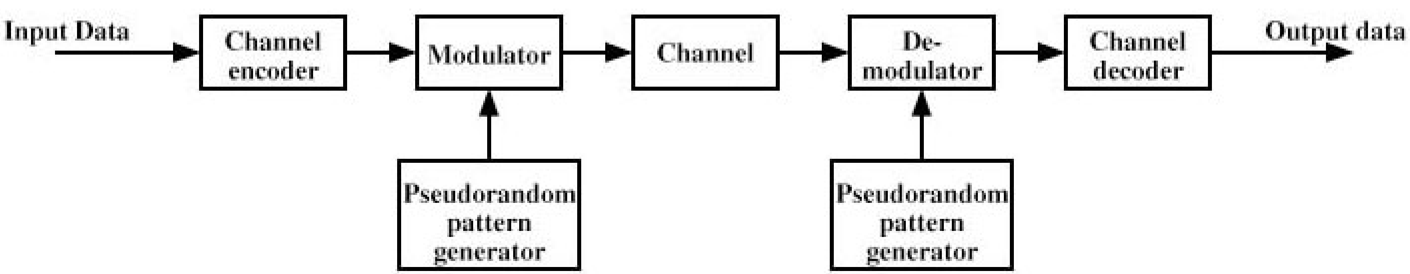


- OQPSK
  - ✓ a variation of QPSK known as offset QPSK or orthogonal QPSK
  - ✓ a delay of one bit time is introduced in the Q stream of QPSK
  - ✓ Its spectral characteristics and bit-error performance are the same as that of QPSK
  - ✓ at any time the phase change in the combined signal never exceeds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

Spread Spectrum

Spread Spectrum is a method of spreading a transmitted spectrum over a wide bandwidth, so that the energy at any particular frequency is not detectable without special foreknowledge of the spreading technique.

- Spread-spectrum transmission offers many advantages over a fixed-frequency transmission.
  - Spread-spectrum signals are highly resistant to narrow band interference
  - Signals are difficult to intercept, so immune to jamming
- **Types**:
  - direct sequence spread spectrum (**DSSS**)
  - frequency hopping spread spectrum (**FHSS**)

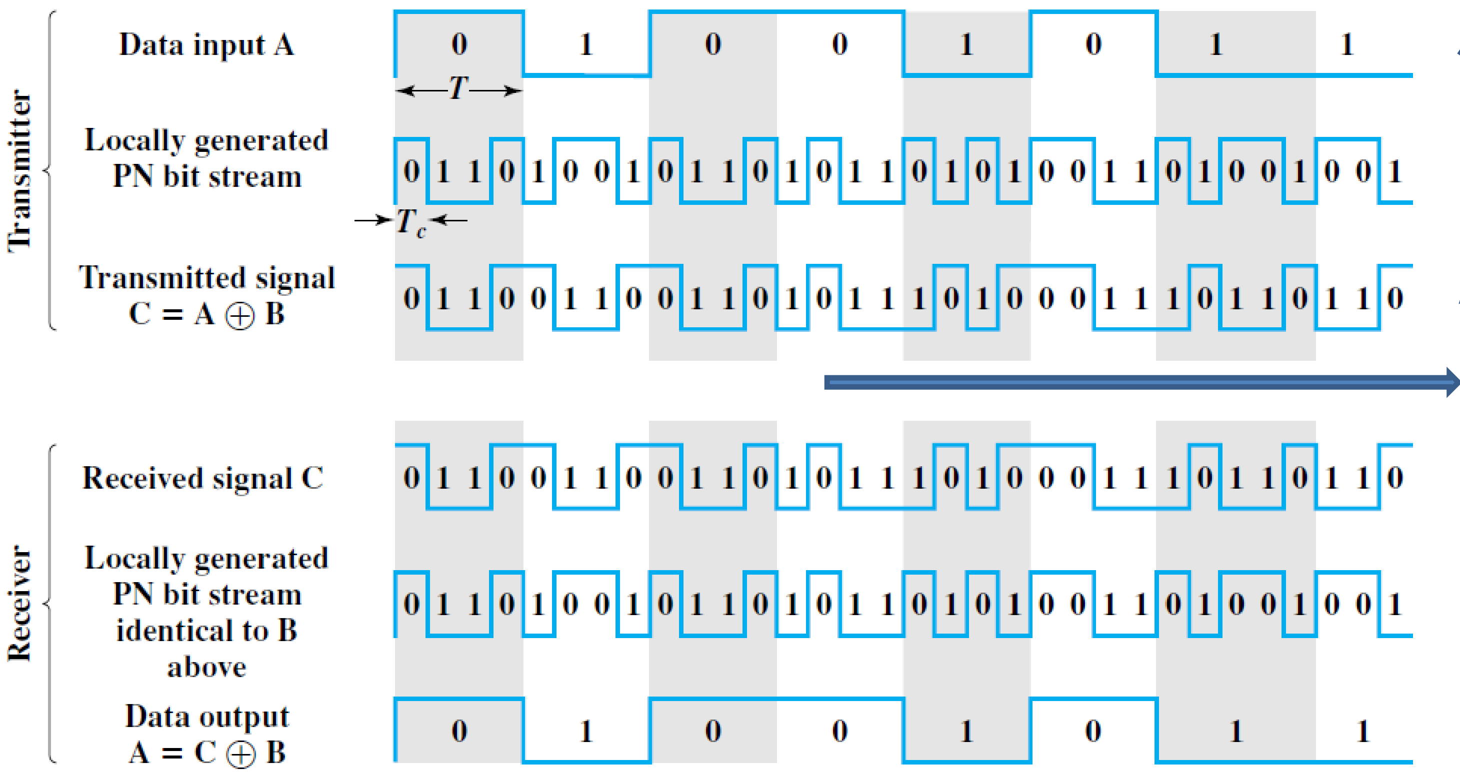


Cont…

- 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

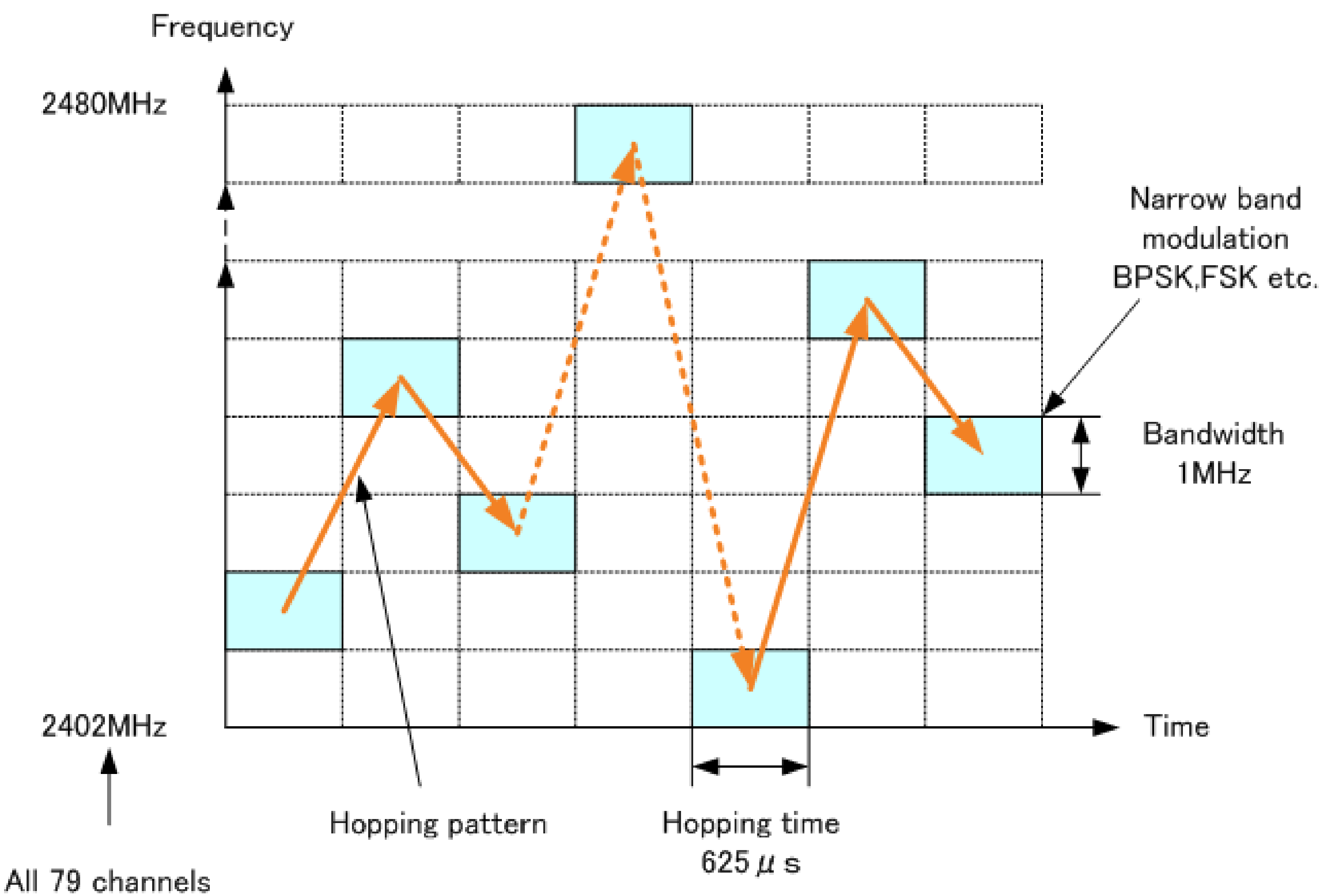


Spread the data stream

Transmit the spread data using modulation

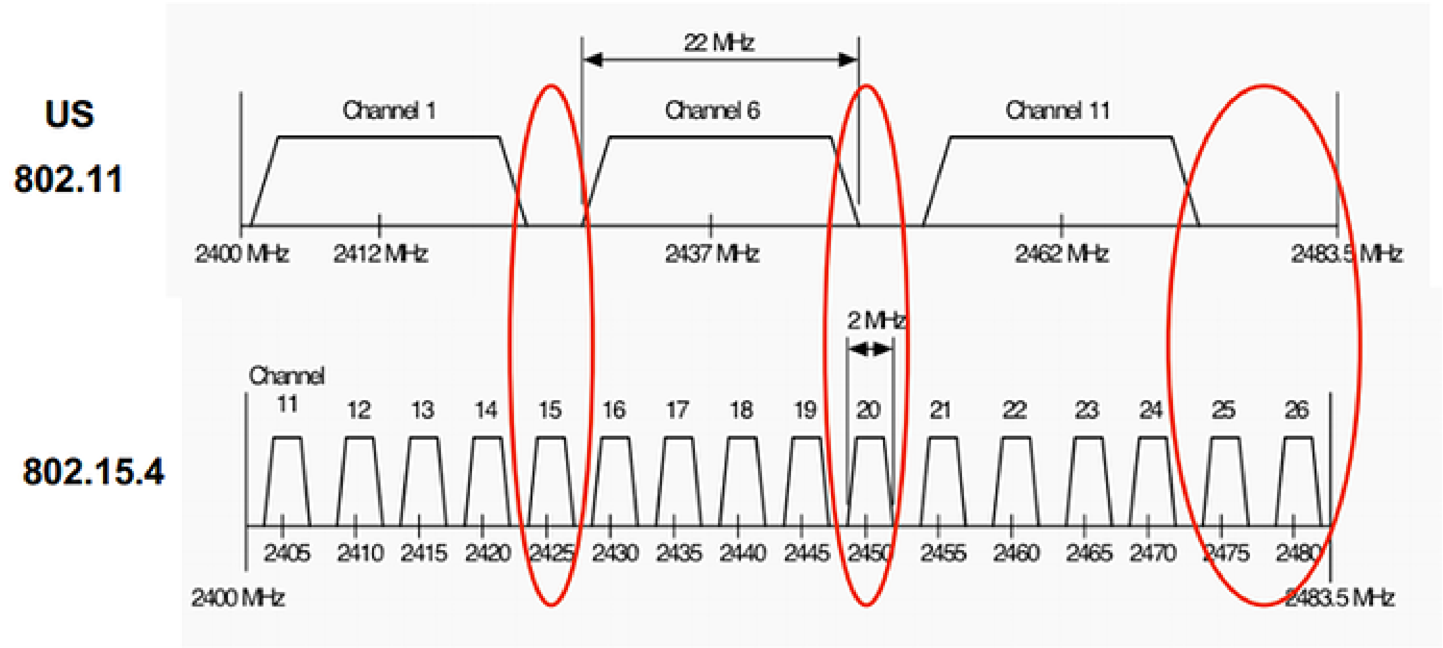
Figure 9.6 Example of Direct Sequence Spread Spectrum

FHSS



Frequency
2480MHz
Narrow band
modulation
BPSK,FSK etc.
Bandwidth
1MHz
2402MHz
Time
Hopping pattern
Hopping time
625 μ s
All 79 channels

Other PHY 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
  - It is an estimate of the received signal power within the bandwidth of the channel
  - 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**
  - The LQI measurement is a characterization of the strength and/or quality of a received packet.
  - The measurement may be implemented using
    i. receiver ED
    ii. signal-to-noise ratio (SNR) estimation, or
    iii. combination of the above methods.
  - Transmitter may decide to use high transmission power based on LQI
  - Applications may dynamically change 802.15.4 channels based on LQI

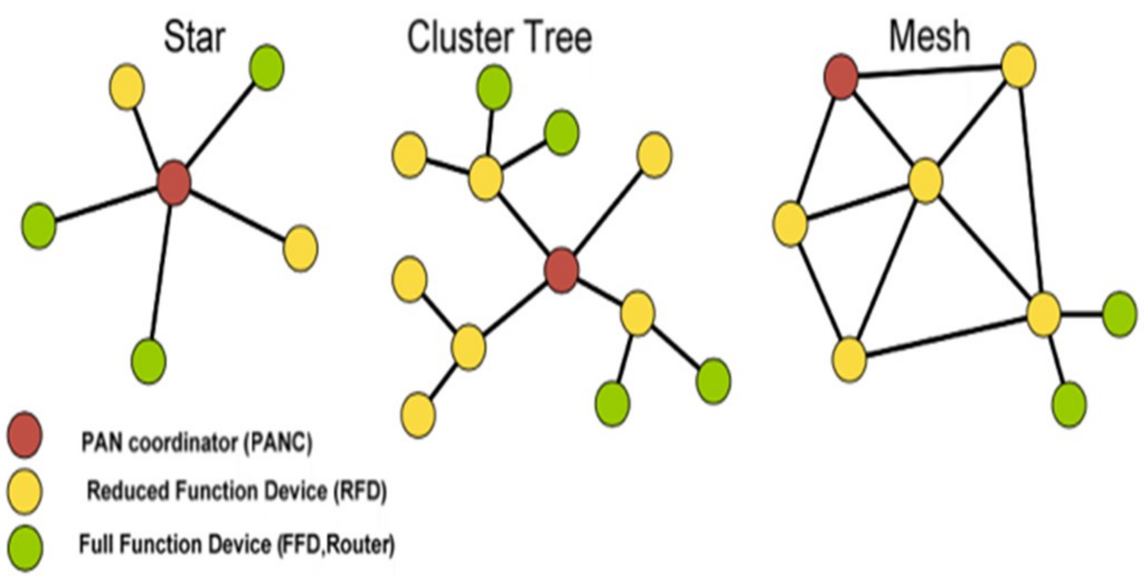
- 802.15.4 uses **CSMA/CA** which ask the PHY layer to do CCA
  - Clear Channel Assessment (CCA) is performed by any one of the below methods:
    - Energy above ED threshold regardless of modulation
    - Carrier sense only (i.e. based on the detection of a signal with modulation and spreading characteristics)
    - Combination of both the above

IEEE 802.15.4 MAC

IEEE 802.15.4 MAC layer

- MAC layer manages access to the PHY channel
  - defines how devices in the same area will share the frequencies allocated.

- Main tasks:
  - Network beaconing for devices acting as coordinators
  - PAN association and disassociation by a device
  - Reliable link communications between two peer MAC entities
  - Device security



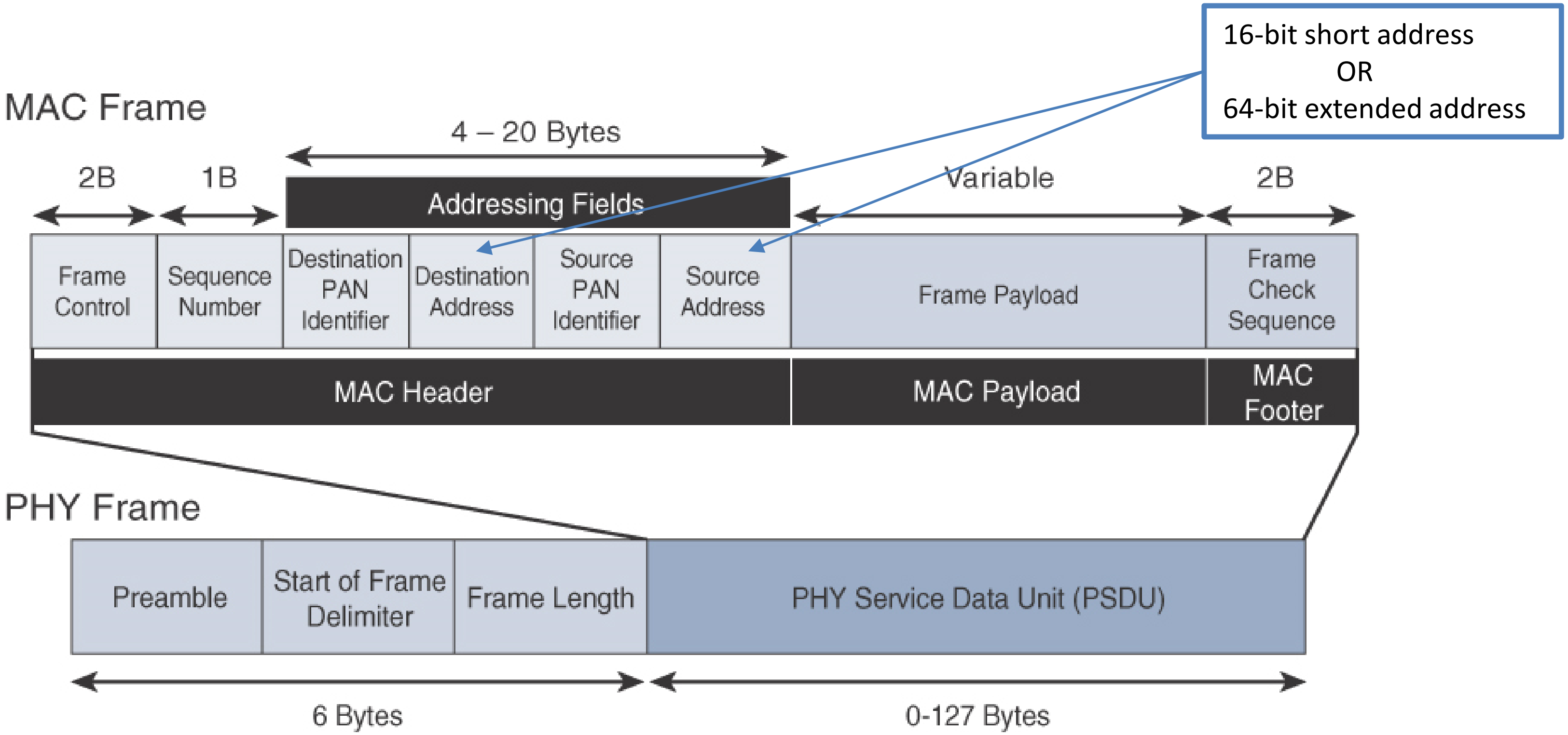
IEEE 802.15.4 Device Types

- 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** (aka Parent, Join Proxy)
    - 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**

General MAC Frame Format



MAC frame types:

- Data frame
- ACK frame
- Beacon frame
- Command frame

Cont...

802.15.4 MAC header						MAC payload
Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable
Frame Control	Sequence number	Destination PAN ID	Destination address	Source PAN ID	Source address	Frame payload

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

-Values of the Frame Type subfield

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

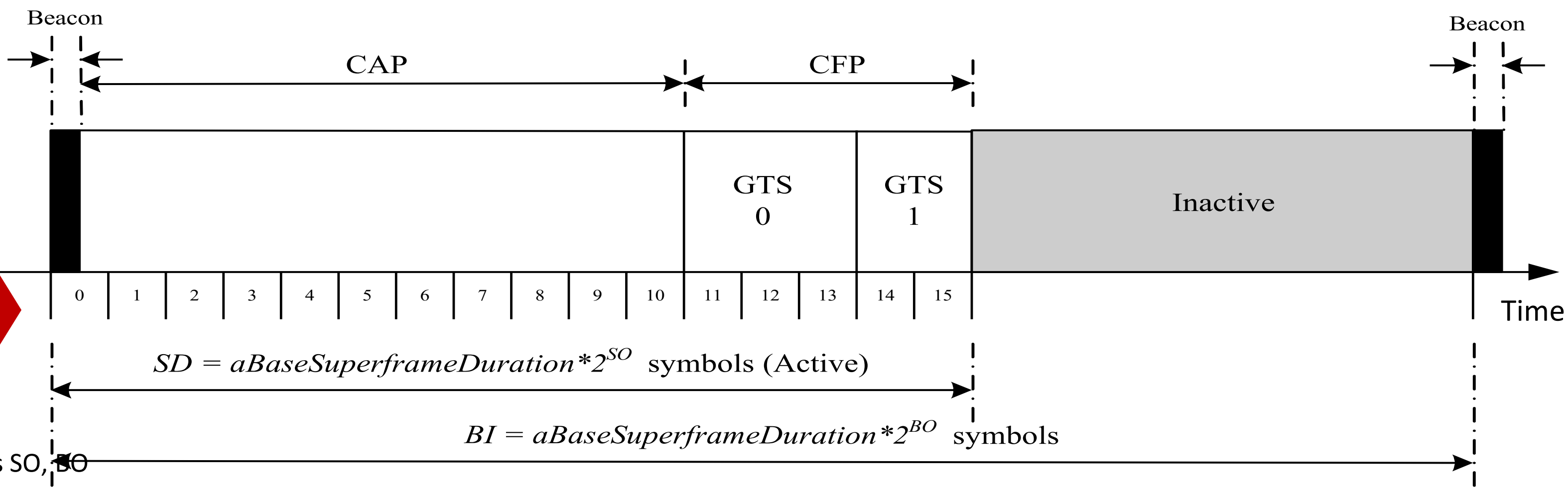
Addressing mode value $b_1\ b_0$	Description
00	PAN identifier and address field are not present.
01	Reserved.
10	Address field contains a 16 bit short address.
11	Address field contains a 64 bit extended address.

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

Superframe



SO: superframe order
BO: beacon order
PAN coordinator decides SO, BO

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

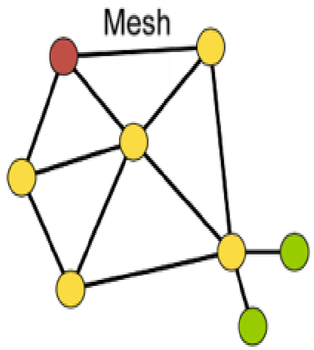
Octets:2	1	4 to 20	variable	2
Frame control	Data sequence number	Address information	Data payload	Frame check sequence
MAC header			**MAC Payload**	**MAC footer**

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 ID



- 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

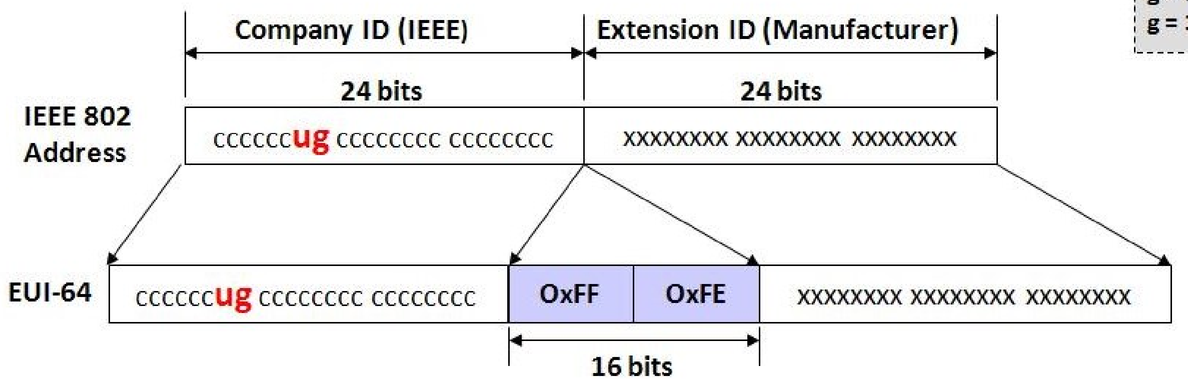
- A device also has a 16-bit short address, which is **allocated by the PAN coordinator** when the device associates with its coordinator.
  - Same short address may be present in to different PAN

- IEEE 802.15.4 devices can be grouped into **PAN.** These are identified by their **2 Byte PAN identifier**

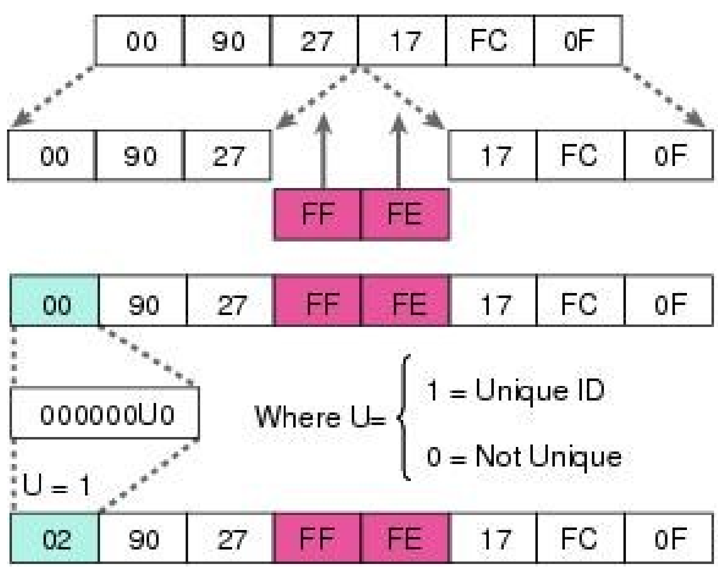
Deriving EUI-64 ID from MAC

Deriving the Modified EUI-64 Interface Identifier from the MAC Address

u = 0 (universal)
u = 1 (local)
g = 0 (individual)
g = 1 (group)



Example:



Addressing Modes

- IEEE 802.15.4 frames contain address of both the source & destination.

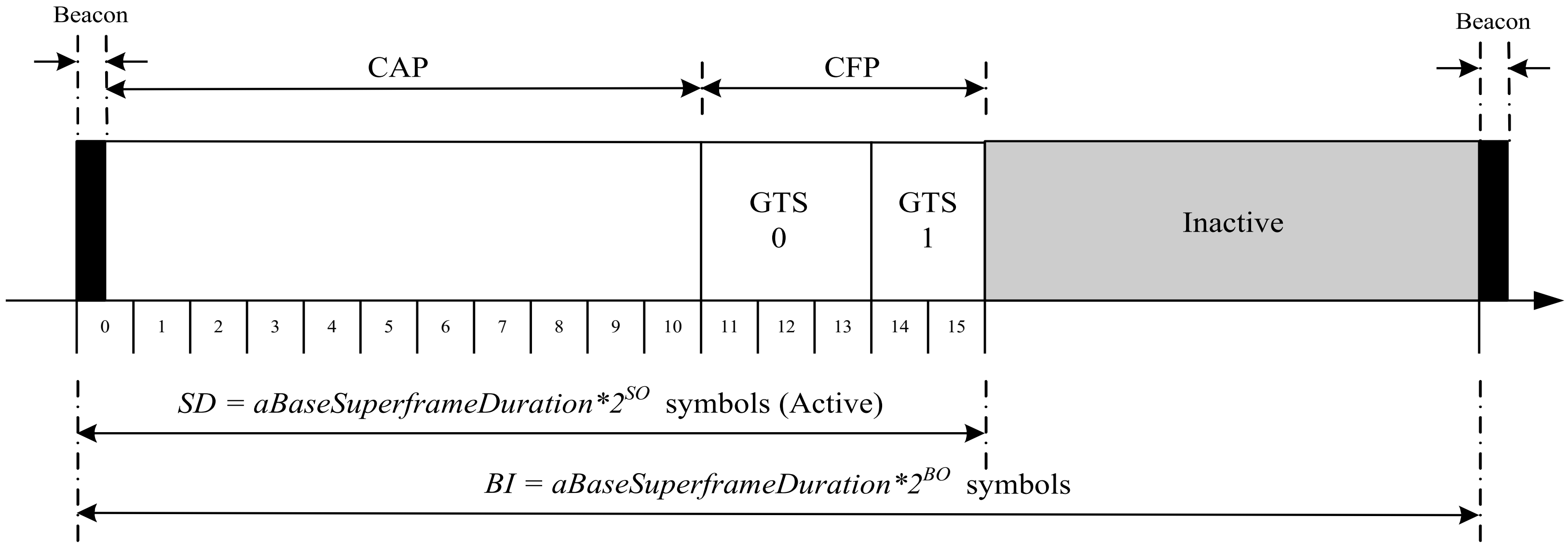
- **Three different addressing modes**, which sets the address field (none/ short/ long, with/without PAN ID)

  – **Short addressing mode**: The address field includes a short address (2B) & a PAN ID (2B) = (total of 4 bytes).

  – **Long addressing mode**: The address field includes a long address (8B) and a PAN ID (2B) = (total of 10 bytes).

  – **No addressing mode**:
    - For ACK frame - both addresses are missing.
    - For *Data* and *Command* frames - only one (either source or destination) field can be omitted
      – if the source address is omitted, it means the PAN coordinator sent the frame;
      – if the destination address is missing, it means it should be received by the PAN 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 in general
    - 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
  - Default value: SO=3, BO=5
- SD: Superframe Duration
- BI: Beacon Interval

Cont…

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

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

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

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

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

Cont…

- In a “beacon-enabled” network (**i.e. uses superframe structure**)
  - Devices use the slotted CAMA/CA mechanism to contend for the channels
  - FFDs who require fixed rates of transmissions can ask for GTS from the coordinator

- In a “nonbeacon-enabled” network (**i.e. do not use superframe structure**)
  - Devices use the unslotted CAMA/CA mechanism for channel access
  - GTS shall not be permitted

- CSMA/CA is not used for Beacon transmission; also not for Data 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

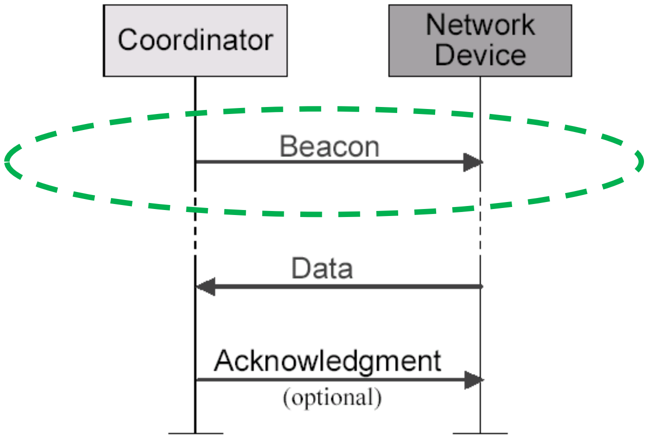
Data Transfer: Device -> Coordinator

In a beacon-enable network

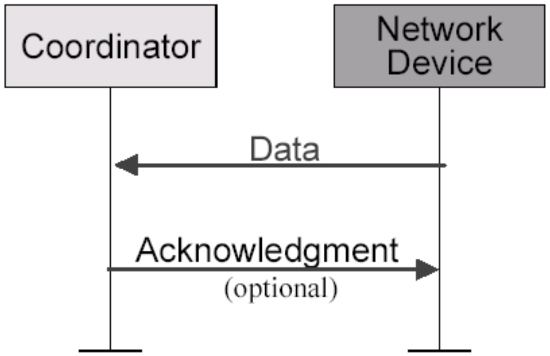
- a device finds the beacon to synchronize to the **superframe** structure.
- Then it uses **slotted CSMA/CA** to transmit its data.

In a non-beacon-enable network

- device simply transmits its data using **unslotted CSMA/CA**



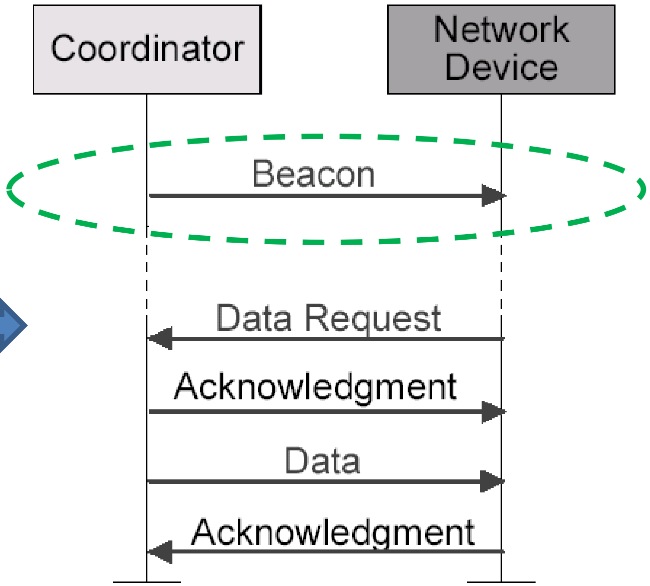
Communication to a coordinator
In a beacon-enabled network

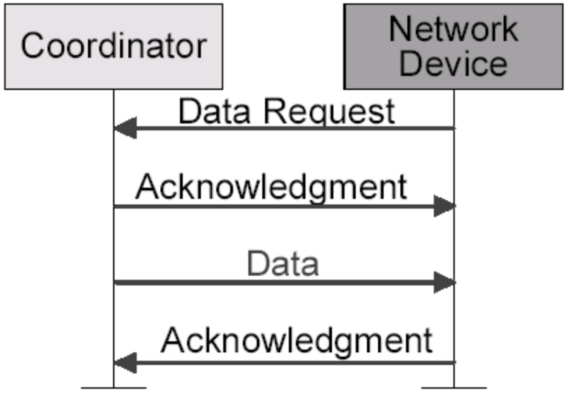


Communication to a coordinator
In a non-beacon-enabled network

Data Transfer: Coordinator -> Device

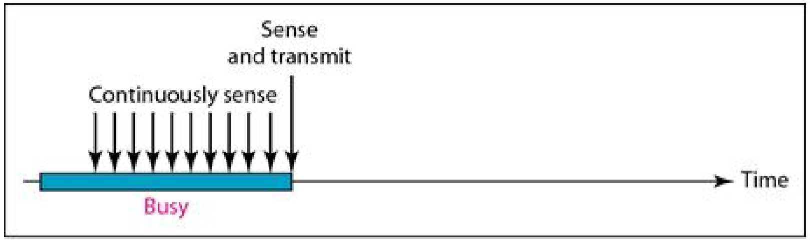
- Data transferred **from** coordinator **to** device
  - in a beacon-enabled network:
    - The coordinator indicates in the **beacon** that some data is pending.
    - A device periodically listens to the beacon and transmits a **Data Request** command using slotted CSMA/CA.
    - Then **ACK**, **Data**,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



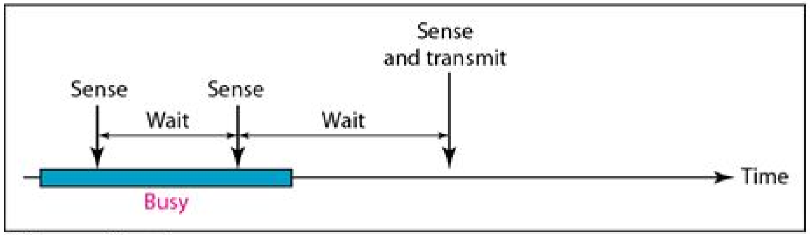


- Data transferred **from** coordinator **to** device
  - in a non-beacon-enable network:
    - The device transmits a **Data Request** using unslotted CSMA/CA.
    - If the coordinator has its pending data, an **ACK** is replied.
    - Then the coordinator transmits **Data** using unslotted CSMA/CA.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

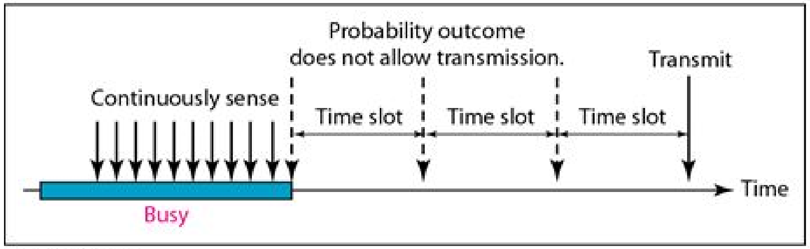
Channel Access Mechanism



a. 1-persistent



b. Nonpersistent



c. p-persistent

- CSMA/CA **random channel access** method
- This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the datalink layer.
- CSMA requires that each station **first check the state of the medium** before sending.
- Persistence methods can be applied to take action when the channel is busy/idle.
  - 1-persistent
    - When station found idle channel, it transmits the frame without any delay.
  - Non-persistent
    - when the channel is found busy, it will wait for the random time and again sense for the state of the station whether idle or busy
  - p-persistent
    - If the channel found to be idle, it transmits the frame with probability p

Slotted CSMA/CA

- CSMA/CA **random channel access**
  - ➢ beacon-enabled network → uses slotted CSMA/CA

In slotted CSMA/CA:

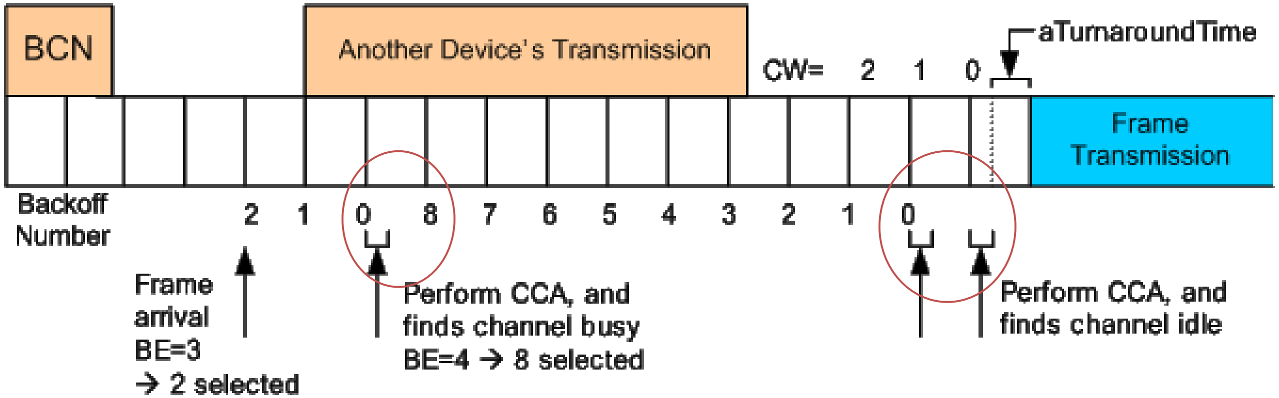
- The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator
  - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
- The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period

Backoff:

- is an algorithm that uses feedback to multiplicatively decrease the rate of some process

Binary exponential backoff (BEB)

- After *c* collisions in BEB algo., the delay is randomly chosen from [0, 1, ..., N] slots, where $N = 2^c - 1$, and expected backoff time (in slots) is N/2.



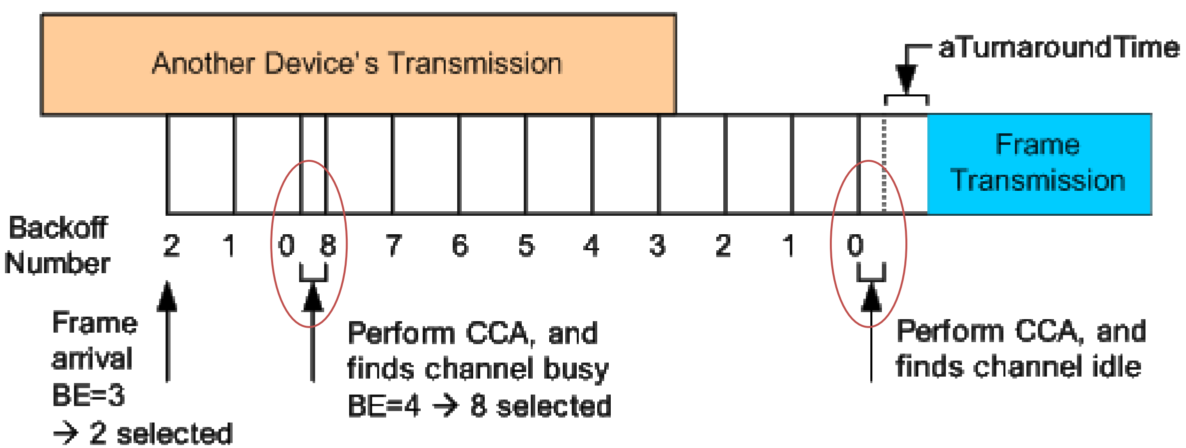
Note:
CW in 802.15.4 is not same with CW in 802.11

Unslotted CSMA/CA

- CSMA/CA **random channel access**
  - ➢ nonbeacon-enabled network → uses unslotted CSMA/CA

In unslotted CSMA/CA:

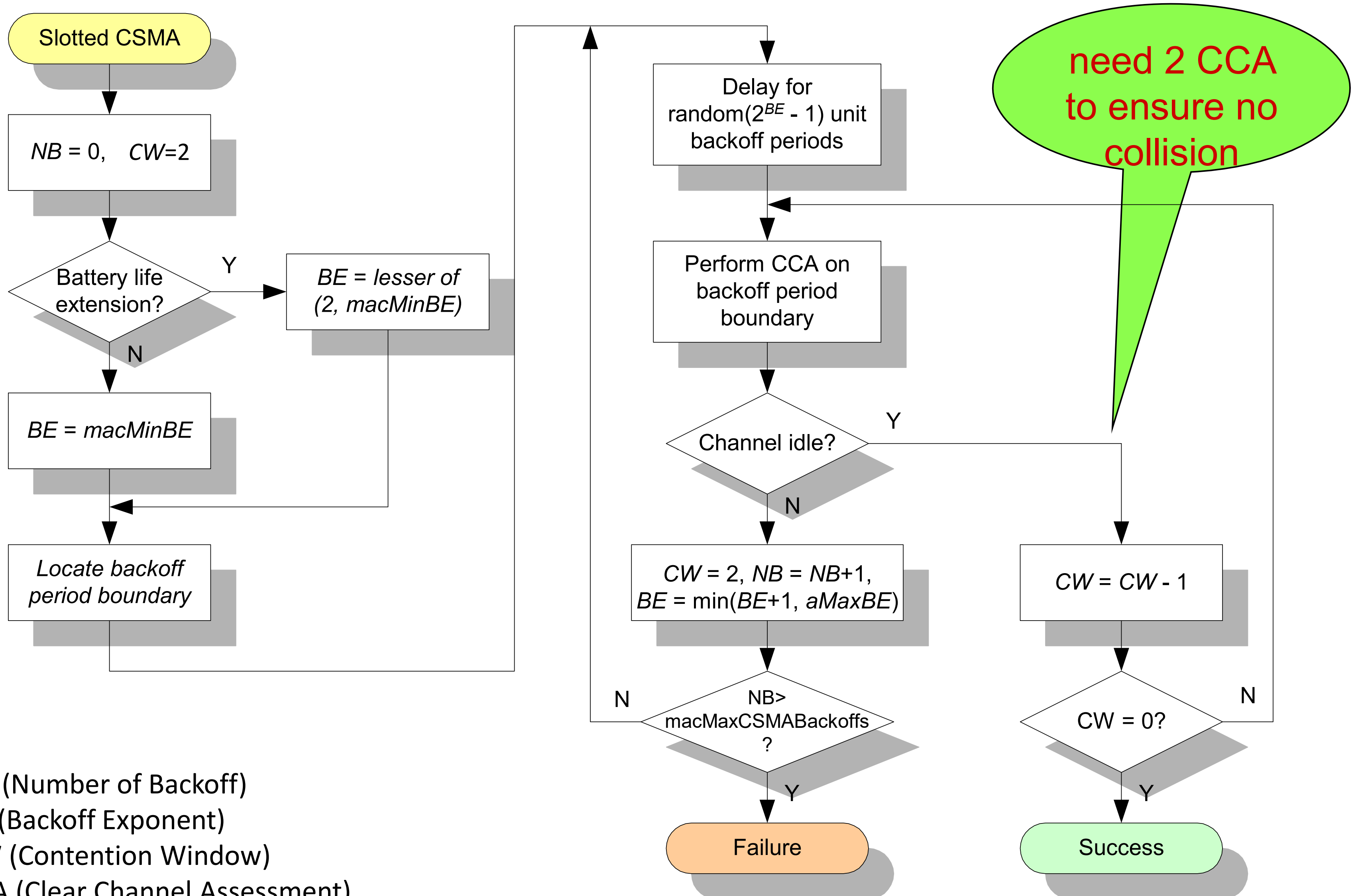
- The backoff periods of one device are not related in time to the backoff periods of any other device in the PAN.
- One backoff period = *aUnitBackoffPeriod*.



Slotted CSMA/CA

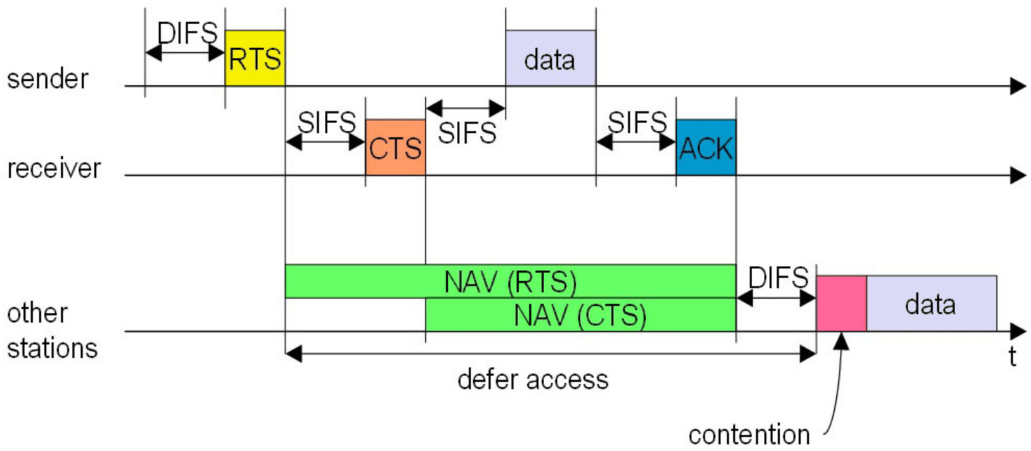
- Each device maintains 3 variables for each transmission attempt
  - NB (Number of Backoff): number of times that backoff has been taken in this attempt of transmission
    - if exceeding macMaxCSMABackoff, the attempt fails
  - BE (Backoff Exponent): play the role to decide how many backoff periods 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
      - Otherwise, 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): 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.
    - Note: CW in 802.15.4 is not same with CW in 802.11
      - CW in 802.11 is used to decide the backoff window from which the backoff period is chosen randomly
      - CW in 802.15.4 is used to decide how many rounds of CCA is required before getting the channel access
- Battery Life Extension (BLE):
  - designed for very low-power operation, where a node only contends in the first few slots

Cont…

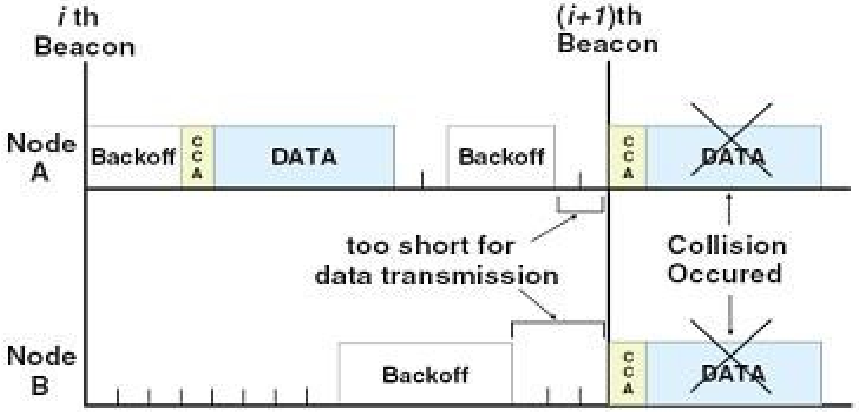


NB (Number of Backoff)
BE (Backoff Exponent)
CW (Contention Window)
CCA (Clear Channel Assessment)

Contention in 802.11 & 802.15.4



Contention in
IEEE 802.11 DCF



Contention in
IEEE 802.15.4
(for slotted CSMA/CA)

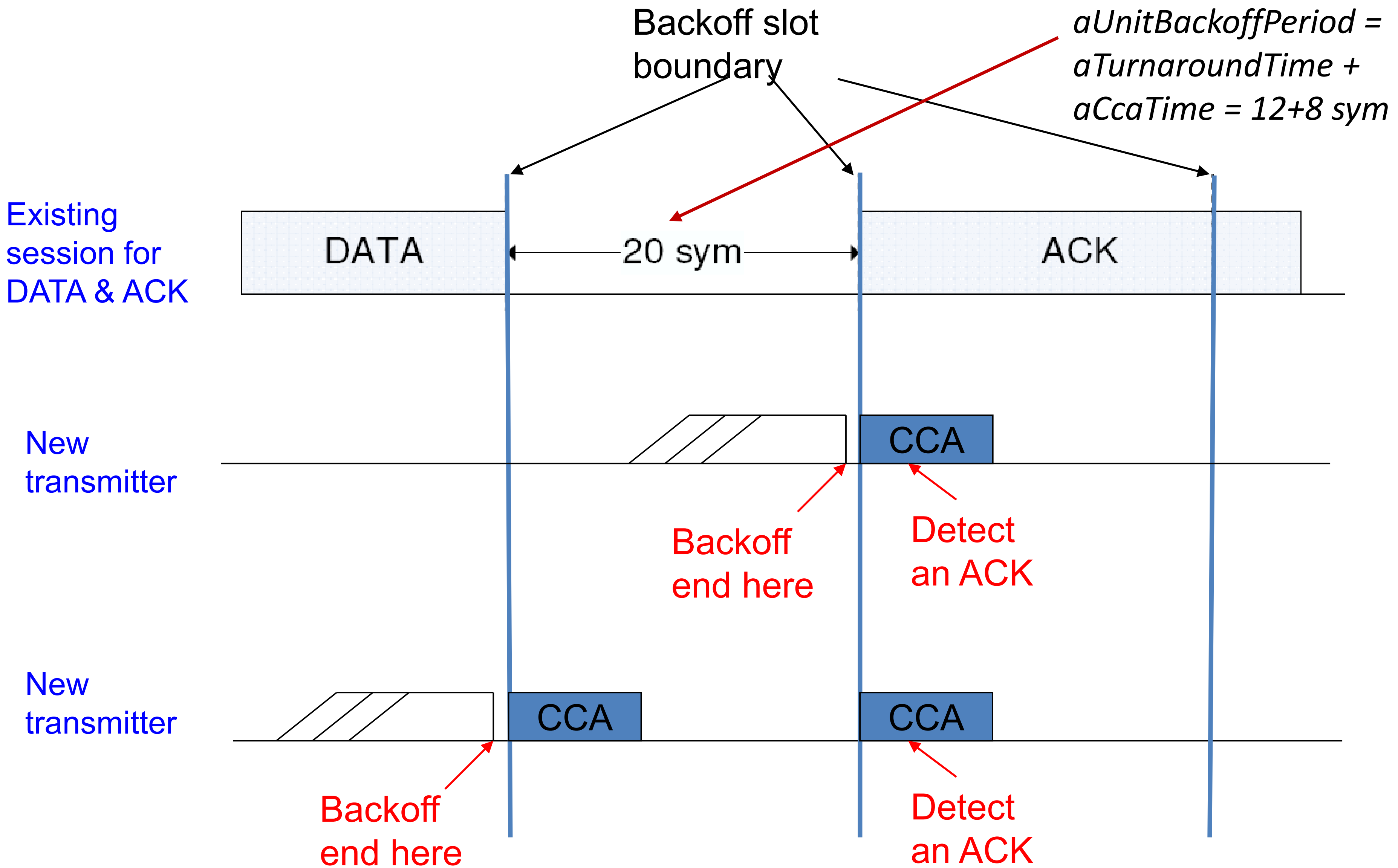
Why 2 CCAs to Ensure Collision-Free

- Each CCA occurs at the boundary of a backoff slot

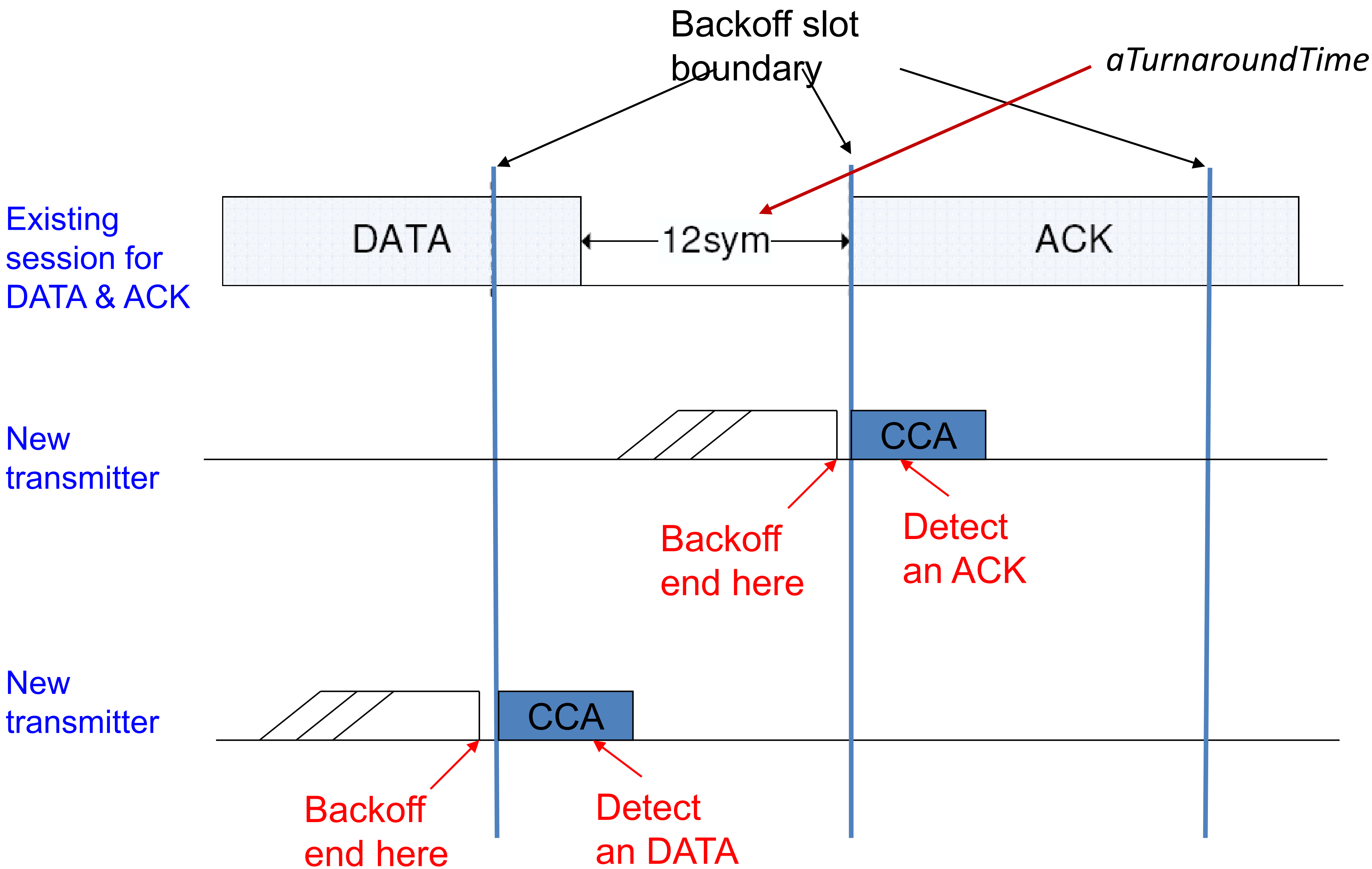
- Each Backoff Slot duration = 20 PHY symbols
- Each CCA duration = 8 PHY symbols

- The standard specifies 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)

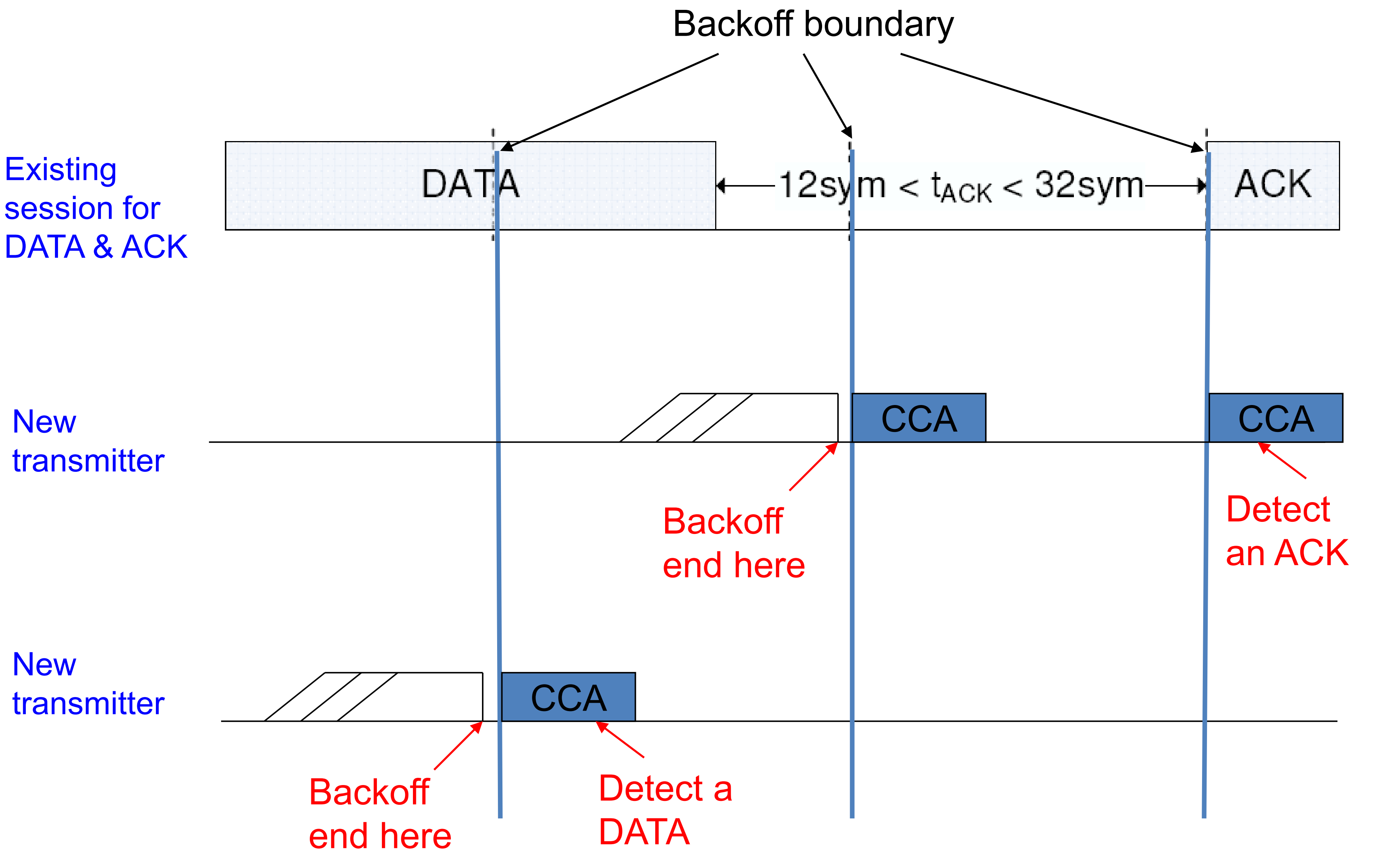
Why 2 CCAs (case 1)



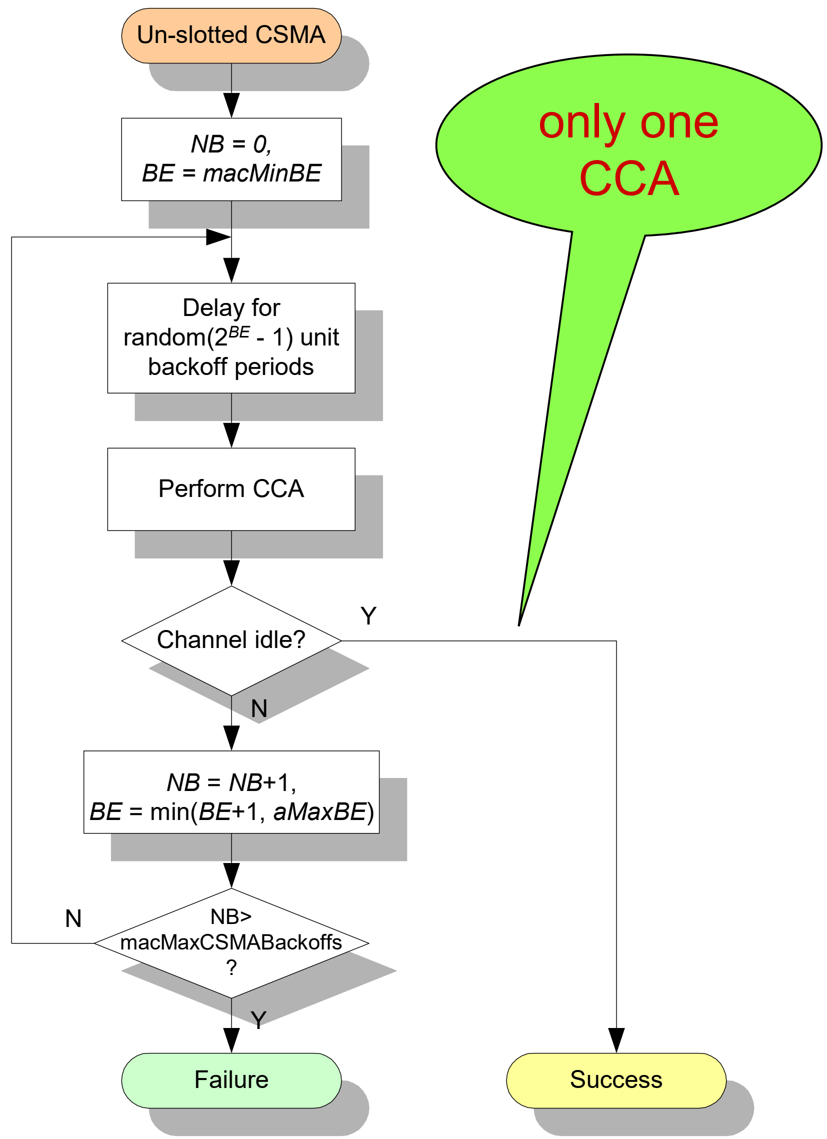
Why 2 CCAs (Case 2)



Why 2 CCAs (Case 3)



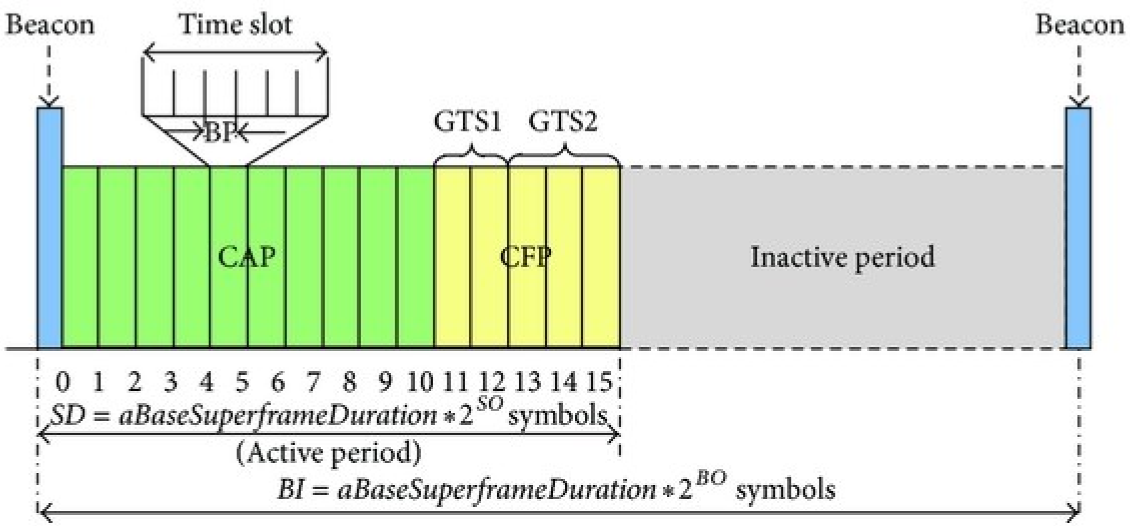
Unslotted CSMA/CA



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

GTS Concepts

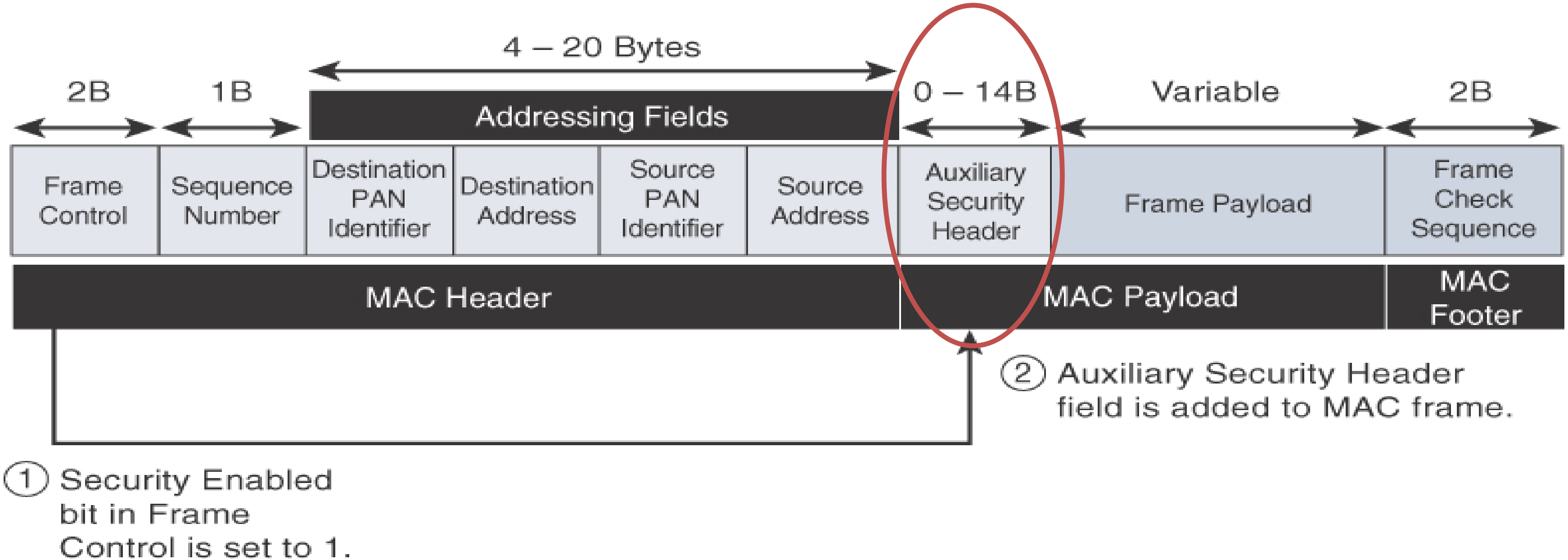
- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe
- A GTS shall only be allocated by the PAN coordinator
- The PAN coordinator can allocated up to 7 GTSs at the same time
- The PAN coordinator decides whether to allocate GTS based on:
  - Requirements of the GTS request
  - The current available capacity in the superframe



Cont…

- 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
- Before GTS starts, the GTS direction shall be specified as either Tx or Rx
  - 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

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 Initial version of IEEE 802.1.5.4**
  - MAC reliability
  - unbounded latency
  - multipath fading

- **IEEE 802.15.4e** amendment of IEEE 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,
    - frequency hopping

- **IEEE 802.15.4g** amendment of IEEE 802.15.4-2011 expands the 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 were needed to support the new PHY

Lessons Learned

- ✓ What is IEEE 802.15.4
- ✓ IEEE 802.15.4. PHY
  - Functionalities
  - Modulation, QPSK, OQPSK
  - Spread Spectrum, DSSS, FHSS
- ✓ IEEE 802.15.4 MAC
  - MAC Frame Formats
  - Timeslot, Superframe
  - Device Addressing
  - Data Transfer Model
  - Channel Access Methods
  - Guaranteed time slot (GTS)
  - Association Procedure
  - Security
- ✓ Limitations of IEEE 802.15.4

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.