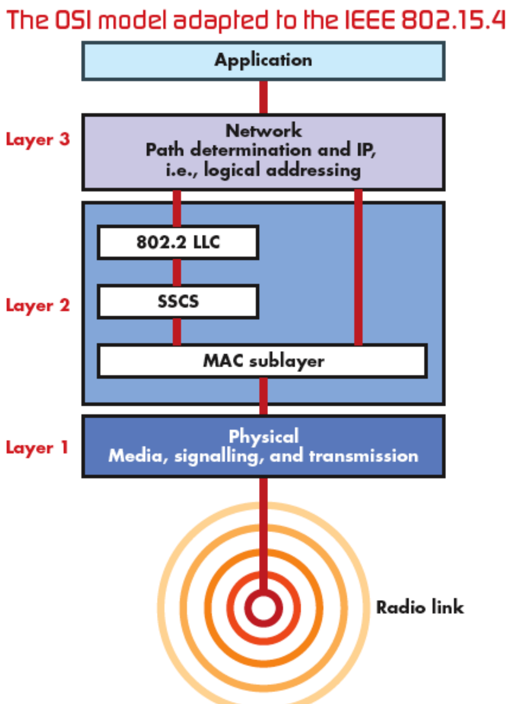
Internet of Things (IoT)

IEEE 802.15.4
Low-Rate Wireless Networks
: MAC Layer

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
Associate Professor
Dept. of CSE, IIT Guwahati
E-mail: manaskhatua@iitg.ac.in

IEEE 802.15.4 Stack – PHY & MAC



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

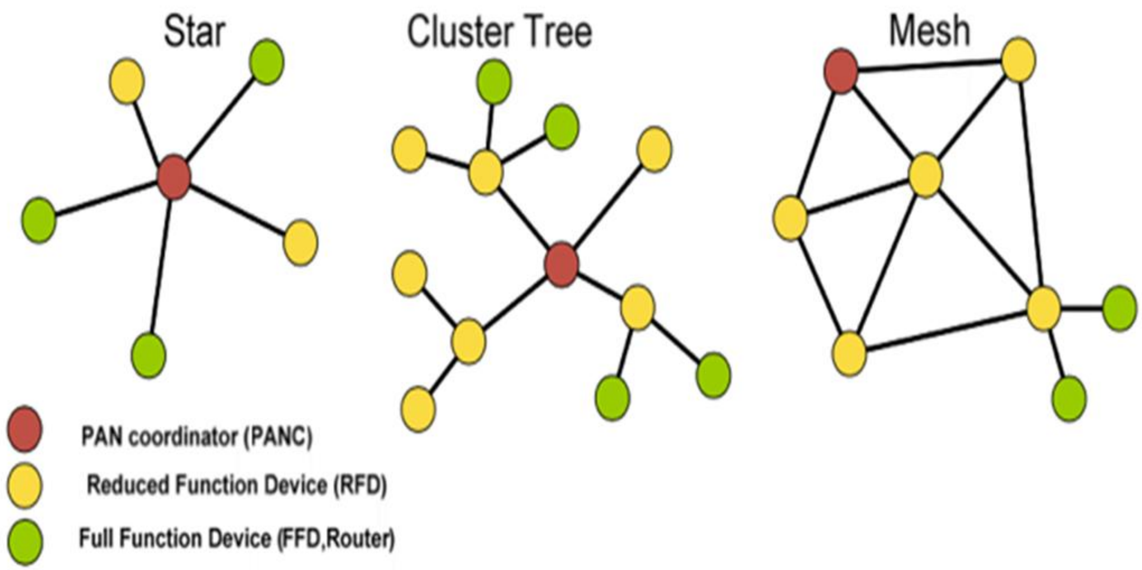
- IEEE 802.15.4 standard is limited to the **PHY & MAC** Layers
- IEEE 802.15.4 standard MAC provides the MAC data service and MAC management services.
  - The **MAC data service** enables transmission of MAC protocol data units (MPDU) across the PHY data service.
  - The **MAC sublayer features** include
    - beacon management,
    - channel access,
    - GTS management,
    - frame validation,
    - ACK frame delivery,
    - association and disassociation,
    - Device security

Standard Document: 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.

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

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.
- MAC layer establish logical topology of the network



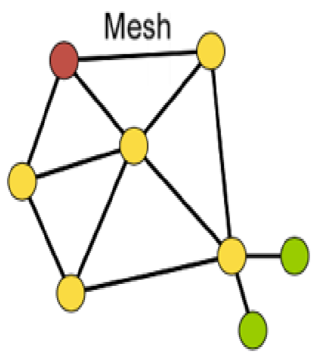
IEEE 802.15.4 Device Types

- 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**

Device Addressing

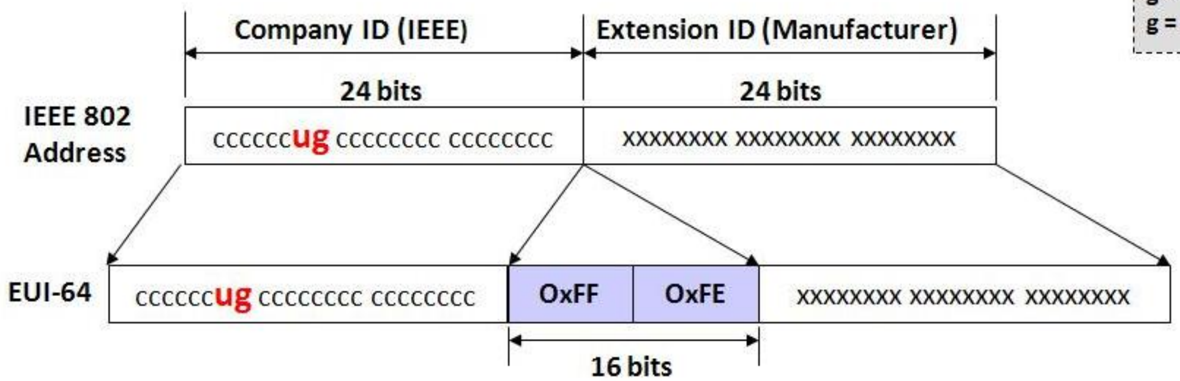


- Two or more devices wirelessly communicating on the same physical channels following IEEE 802.15.4 constitute a PAN.
  - A PAN includes at least one FFD (PAN coordinator)
  - Each independent PAN will select a unique PAN ID
  - PAN ID is generally of 2 bytes
- Each device operating on a network has a unique 64-bit address
  - called extended unique identifier (EUI-64)
  - This address can be used for direct communication in the PAN
  - This is also called 64-bit long address
  - Generally, it is autogenerated from unique MAC address
- A device also has a 16-bit short address, which is allocated by the PAN coordinator when the device associates with its coordinator.
  - Note: Same short address may be present into different PAN

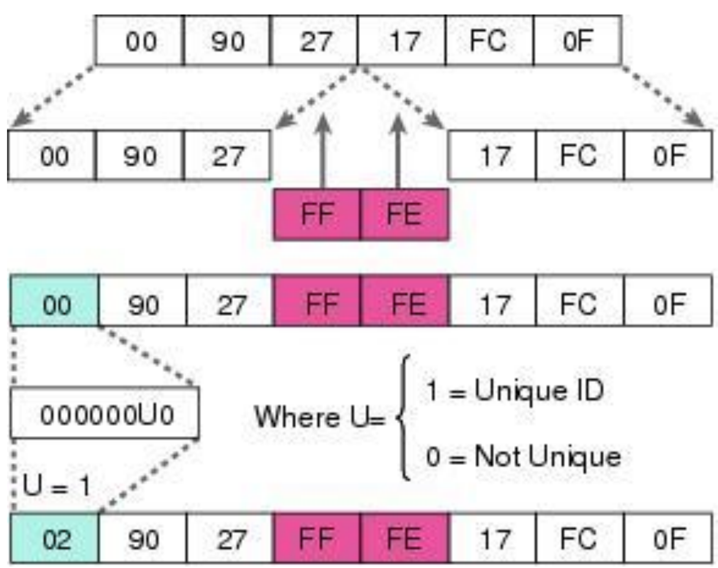
Deriving EUI-64 ID from MAC

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.

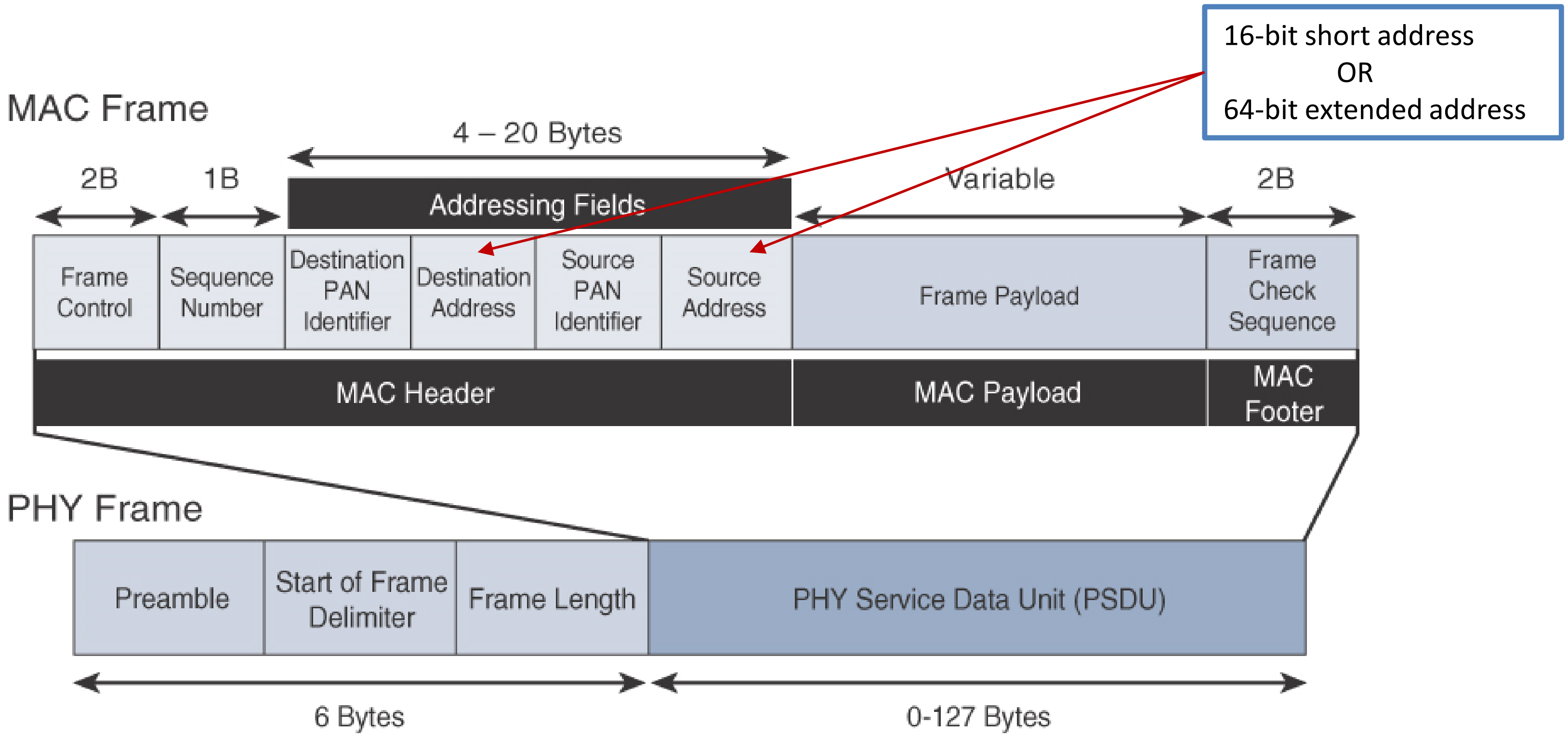
- **Three different addressing modes**, which sets the address field (none/ short/ long, with/without PAN ID)

  - **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.

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

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

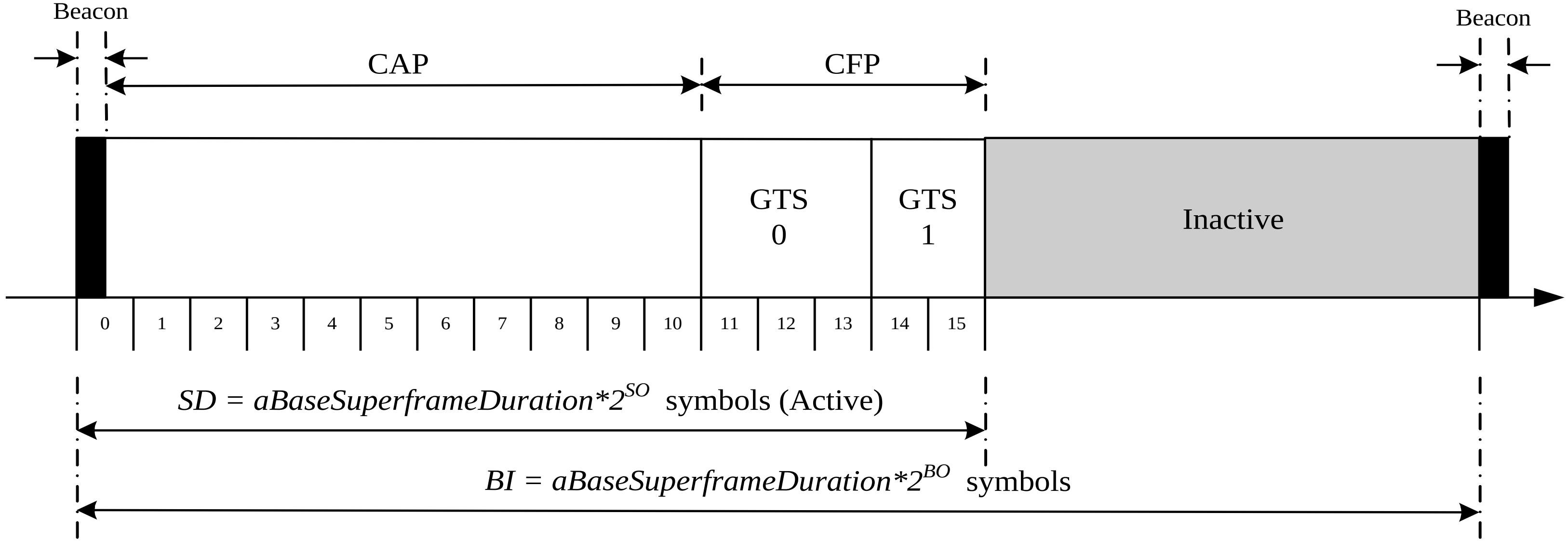
Data Frame

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**

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

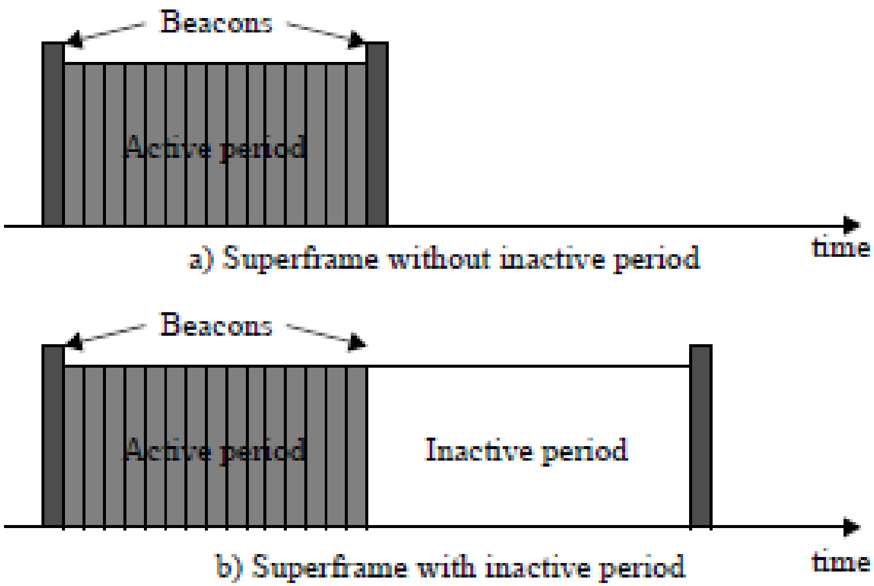
  = can range from 15.36 *msec* to 215.7 *sec* (= 3.5 min).

- 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

Beacon Superframe and GTS



Beacon Enabled Superframe

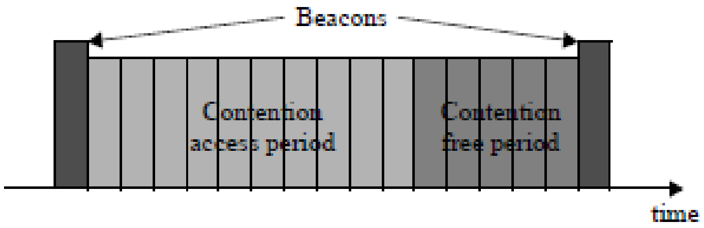


Figure 5-6—Structure of the active periods with GTSs

Active Periods with GTS

Beaconed / Non-beaconed network

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

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

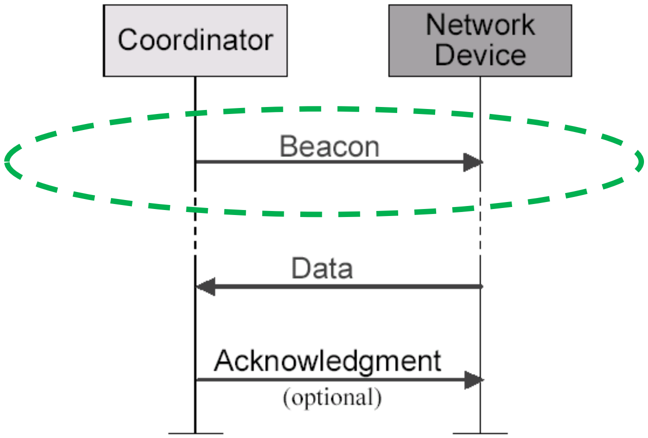
Data Transfer: Device -> Coordinator

In a beacon-enable network

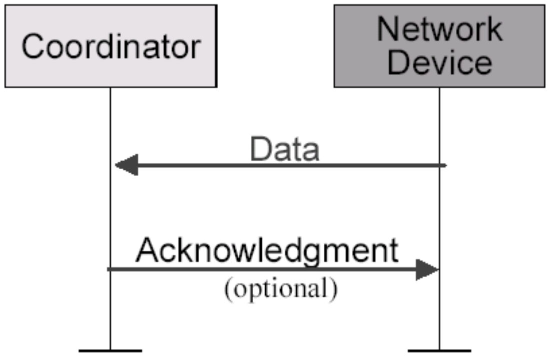
- a device finds the beacon to synchronize to the **superframe** structure.
- Then it uses **slotted CSMA/CA** to transmit its data.

In a non-beacon-enable network

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



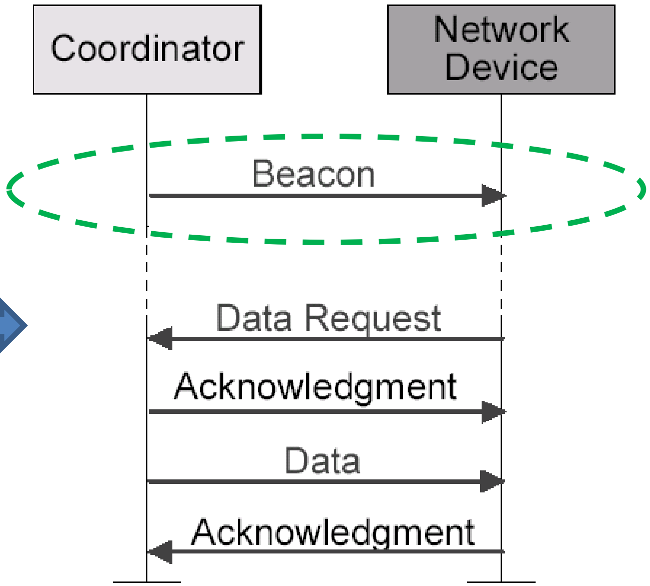
Communication to a coordinator
In a beacon-enabled network

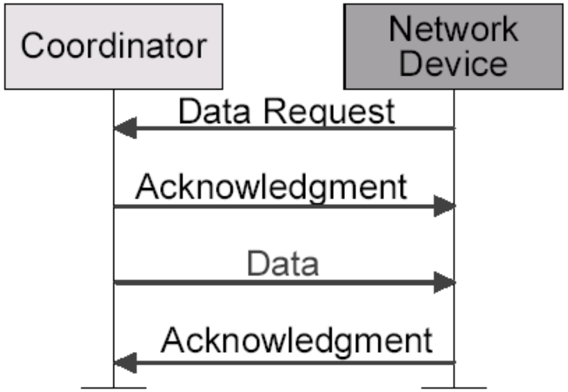


Communication to a coordinator
In a non-beacon-enabled network

Data Transfer: Coordinator -> Device

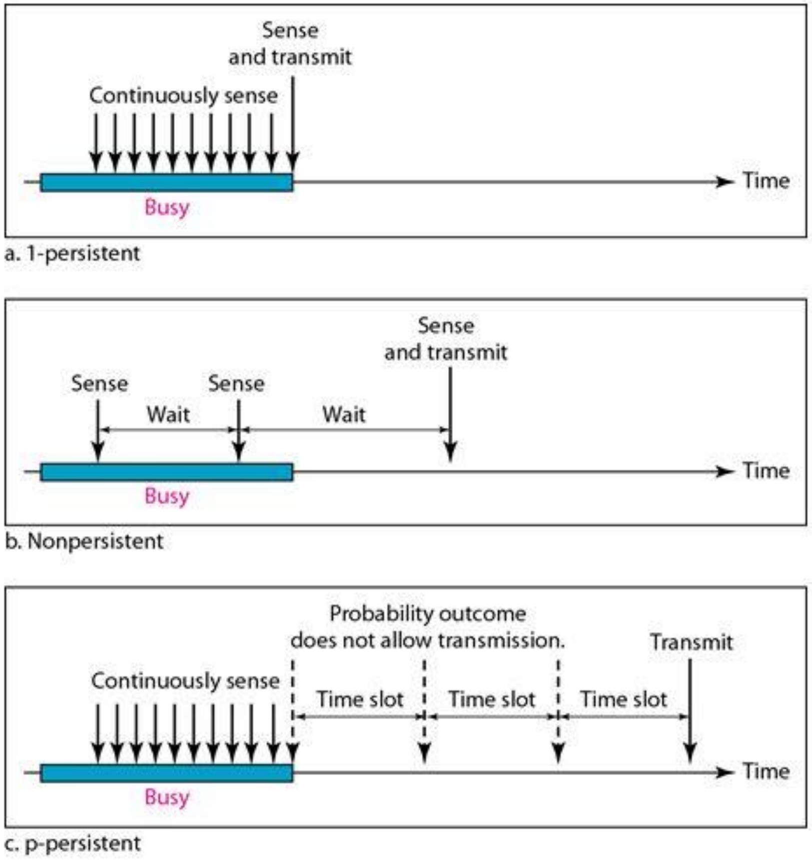
- Data transferred **from** coordinator **to** device
  - in a beacon-enabled network:
    - The coordinator indicates in the **beacon** that some data is pending.
    - A device periodically listens to the beacon and transmits a **Data Request** command using slotted CSMA/CA.
    - Then **ACK**, **Data**,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



- **CSMA** requires that each station first check the state of the medium before sending.
- This method aims to decrease the chances of collisions when two or more stations want to transmit data
- **Persistent** methods can be applied to take action when the channel is sensed 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
    - This is implemented using backoff period concept

Unslotted CSMA/CA

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

In unslotted CSMA/CA:

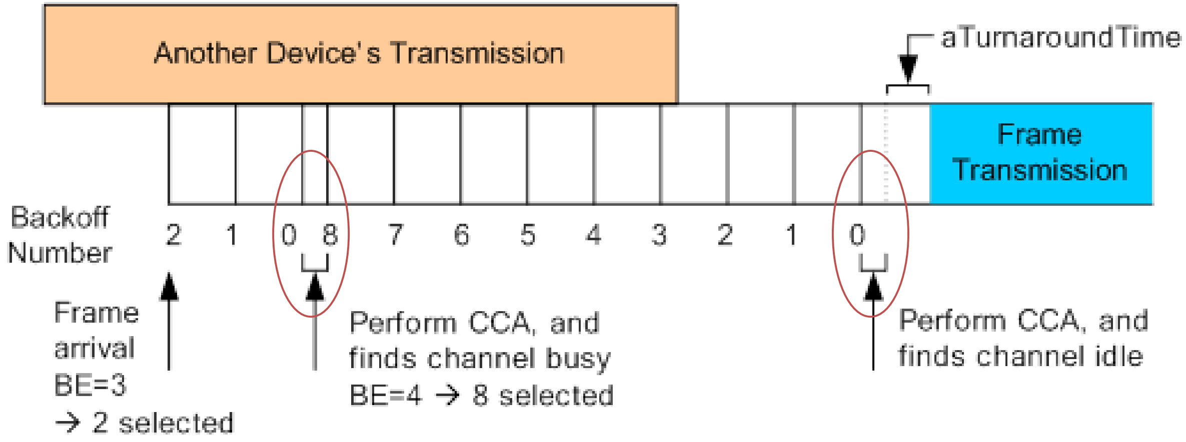
- The backoff periods of one device are not related in time to the backoff periods of any other device in the PAN.
- One backoff period = *aUnitBackoffPeriod*.

Backoff:

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

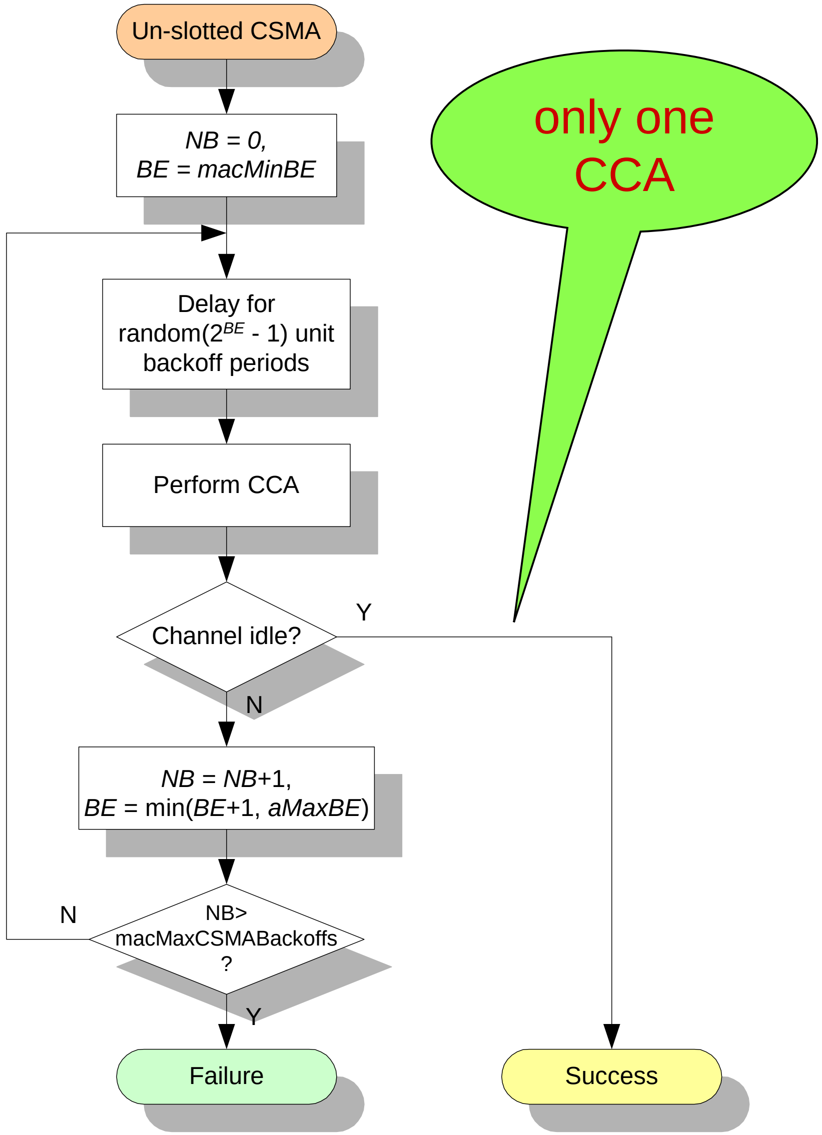
Binary exponential backoff (BEB)

- After *c* collisions in BEB algo., the delay is randomly chosen from [0, 1, ..., N] slots, where $N = 2^c - 1$.



BE: Backoff Exponent

Cont…



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.

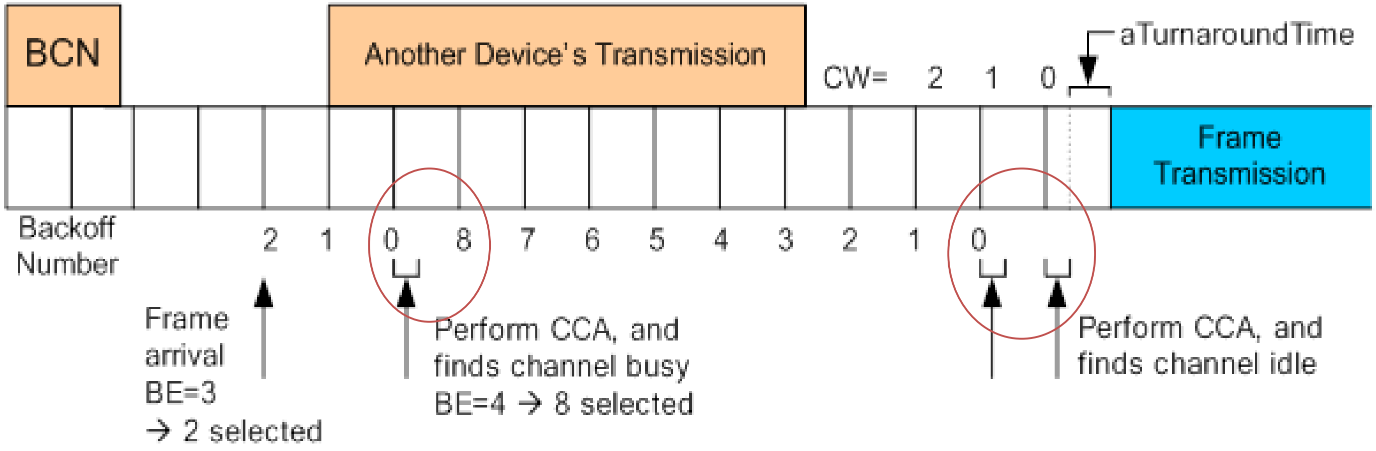
CCA (Clear Channel Assessment)

Slotted CSMA/CA

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

In slotted CSMA/CA:

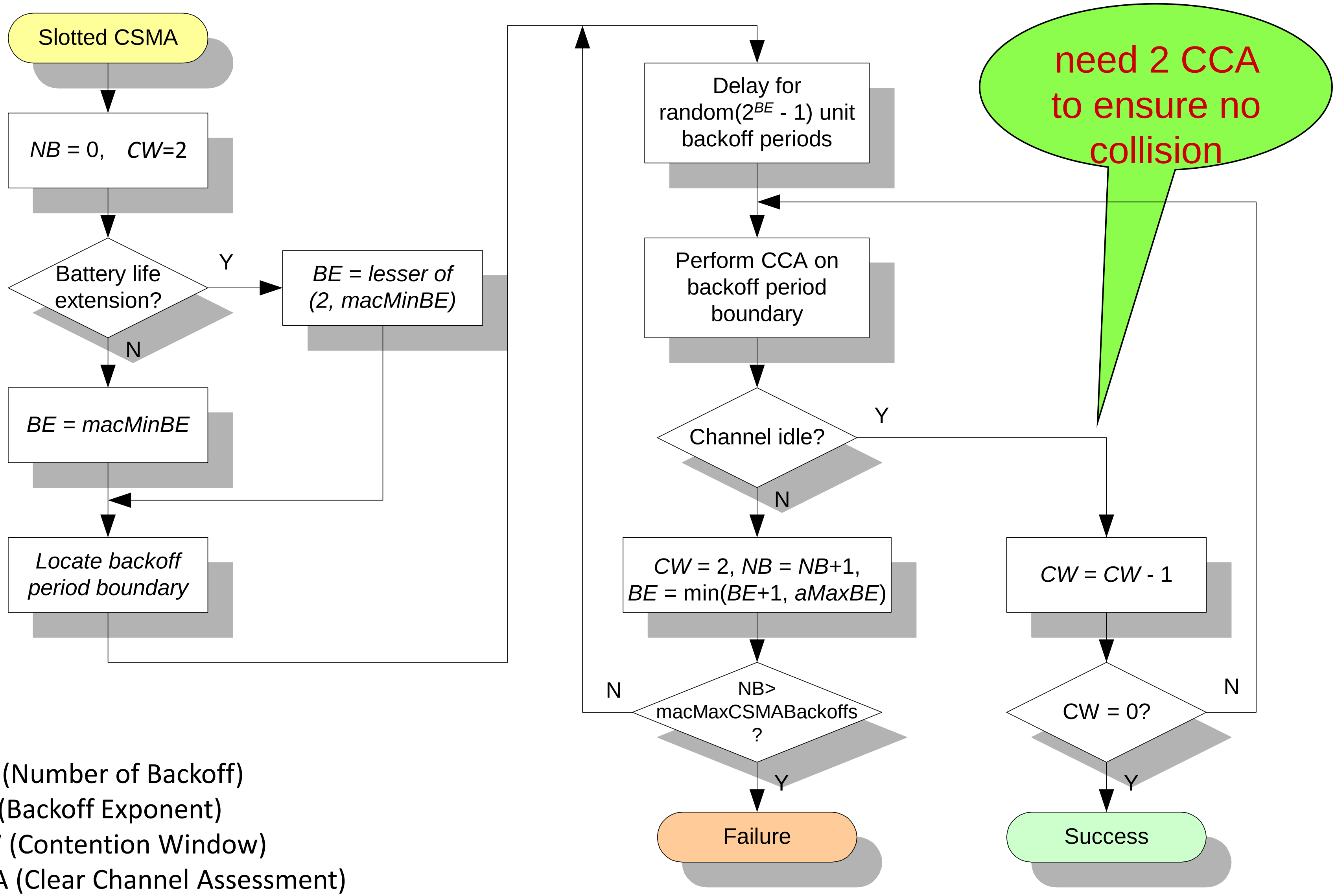
- The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator
  - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
- The MAC sublayer shall ensure that the PHY layer commences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



Cont…

- 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 lesser than the remaining number of slots 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 size 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)

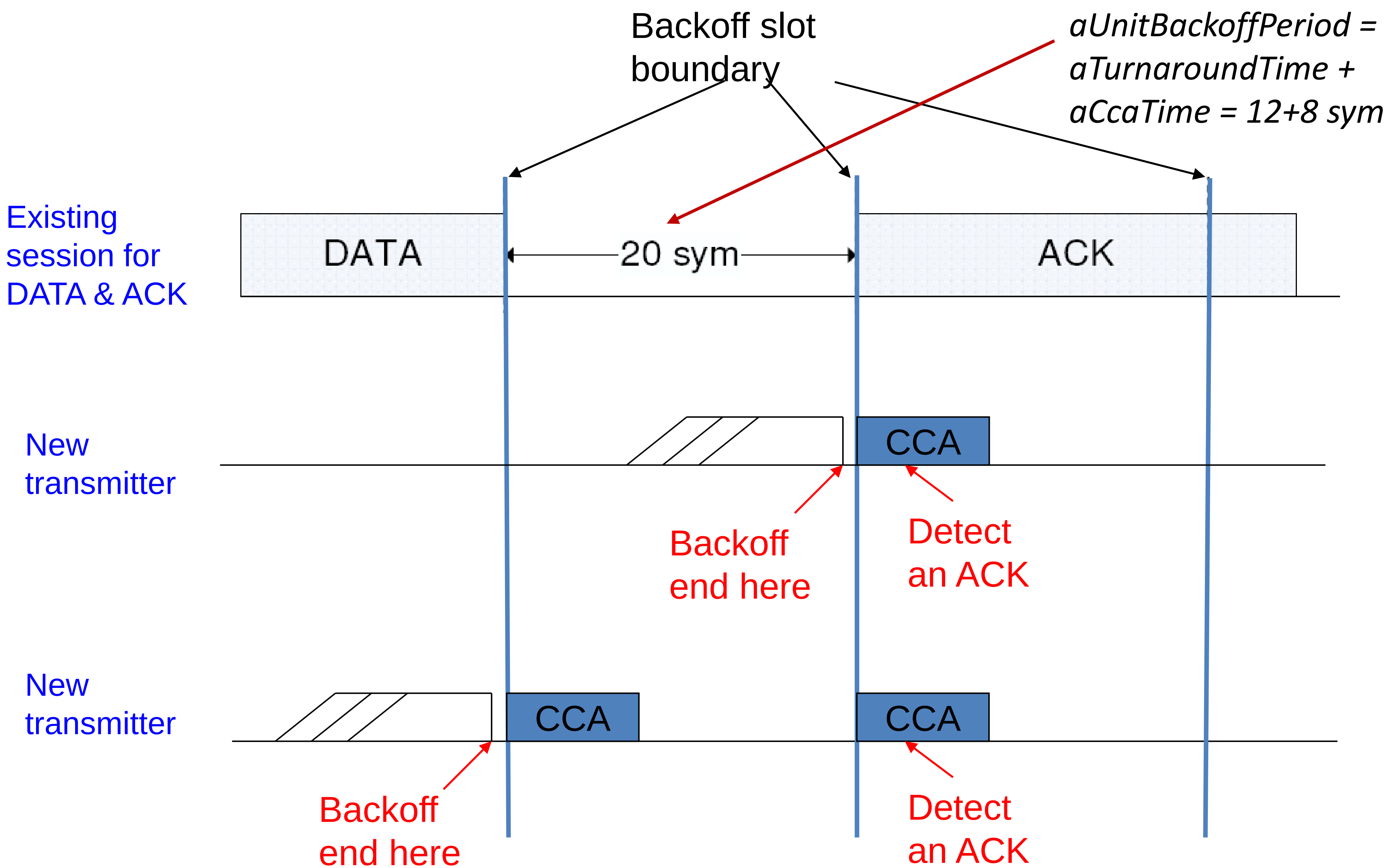
Why 2 CCAs to Ensure Collision-Free

- Each CCA occurs at the boundary of a backoff slot

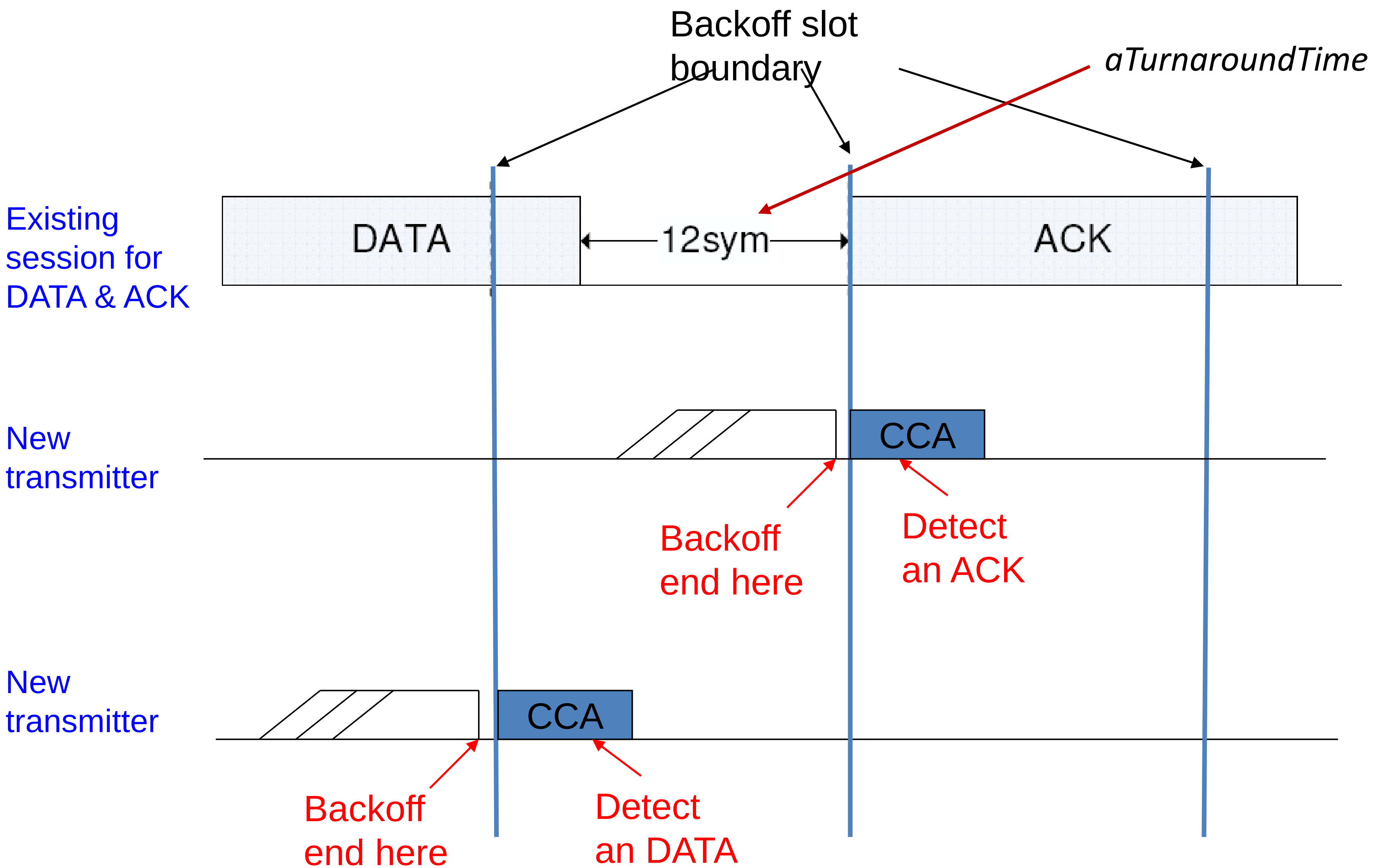
- Each Backoff Slot duration = 20 PHY symbols
- Each CCA duration = 8 PHY symbols

- 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)

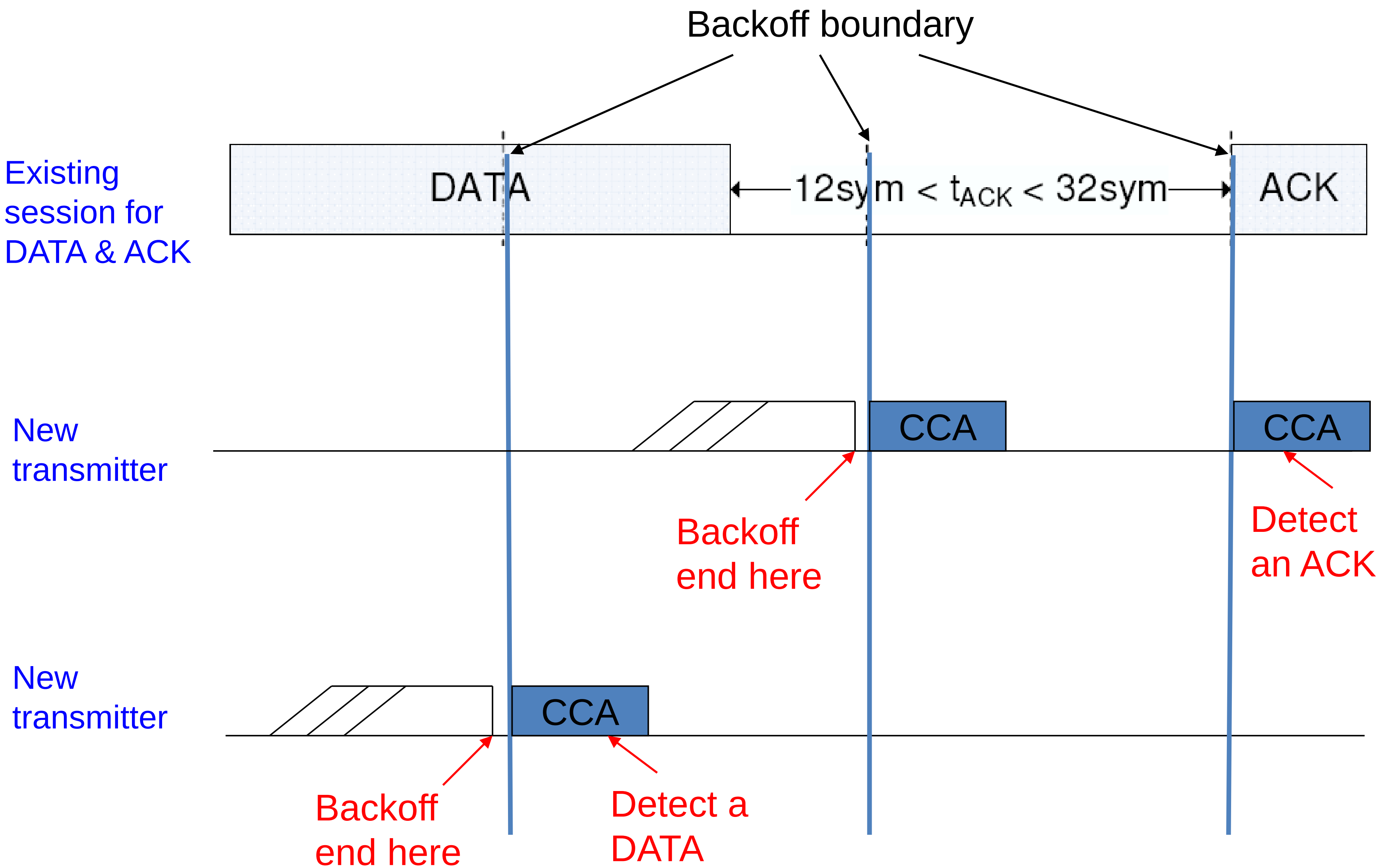
Why 2 CCAs (case 1)



Why 2 CCAs (Case 2)

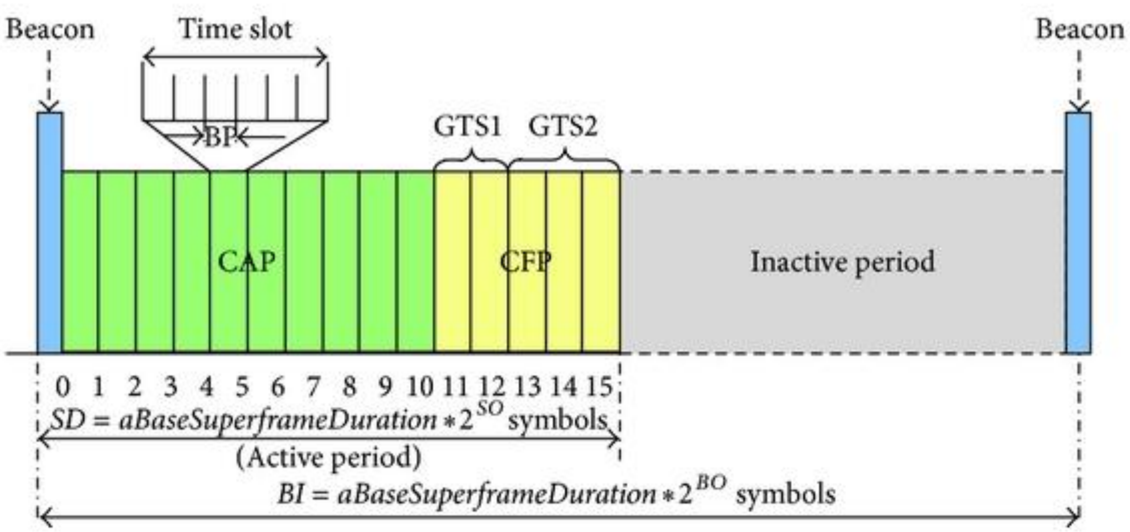


Why 2 CCAs (Case 3)



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 allocate 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

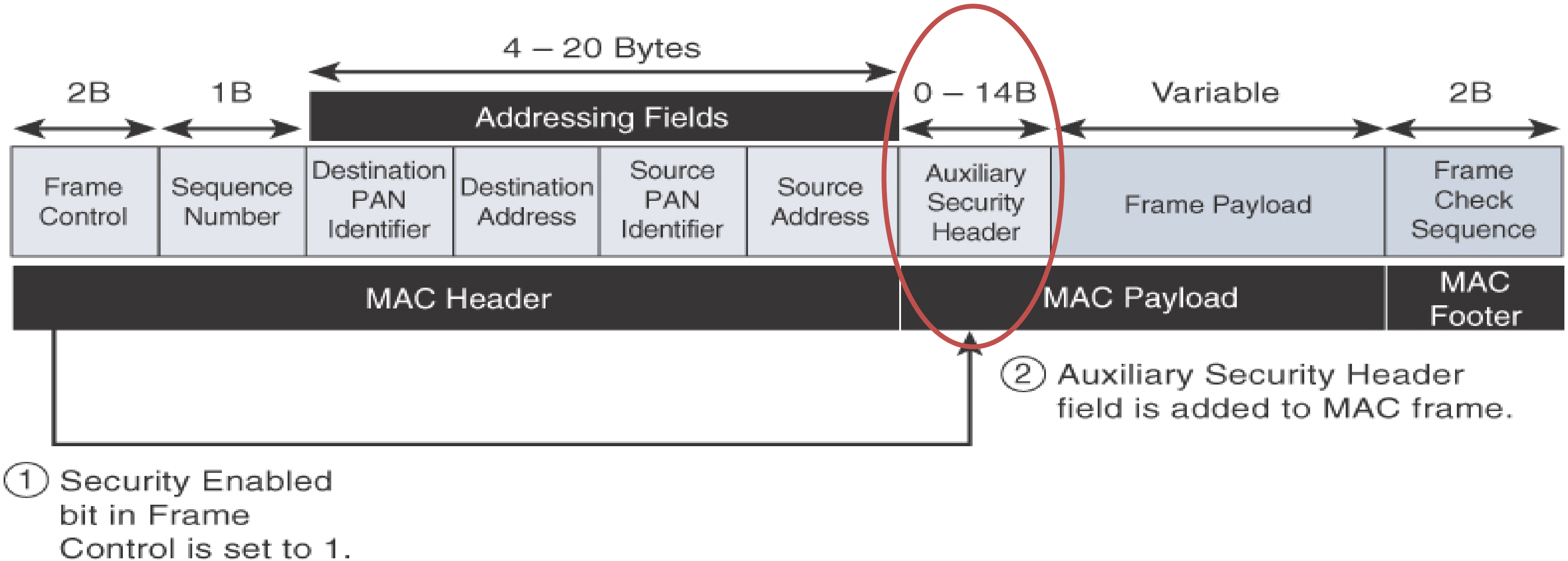
- Before GTS starts, the GTS direction shall be specified as either Tx or Rx
  - Each device may request one transmit GTS and/or one receive GTS

- 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

- ✓ IEEE 802.15.4 MAC
  - Network Topology
  - Device Types
  - Device Addressing
  - MAC Frame Formats

  - Timeslot, Superframe
  - Data Transfer Model

  - Channel Access Methods
  - Slotted CSMA/CA

  - Guaranteed time slot (GTS)
  - Association Procedure
  - Security

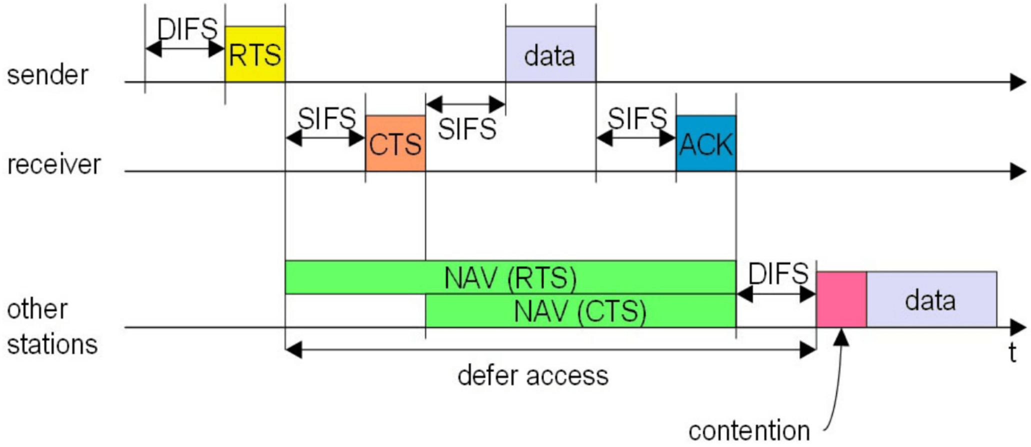
- ✓ Limitations of IEEE 802.15.4

Thanks!

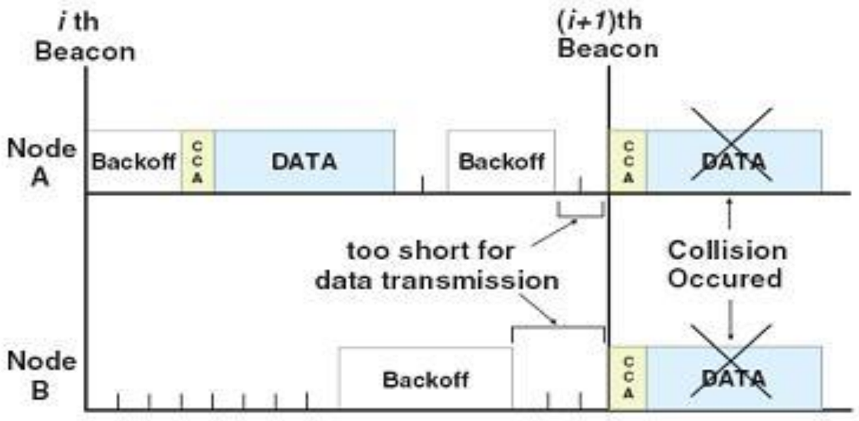
Figures and slide materials are taken from the following sources:

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.

Contention in 802.11 & 802.15.4



Contention in IEEE 802.11 DCF



Contention in IEEE 802.15.4 (for slotted CSMA/CA)