

IEEE 802.15.4

ZigBee PHY and DLL layers

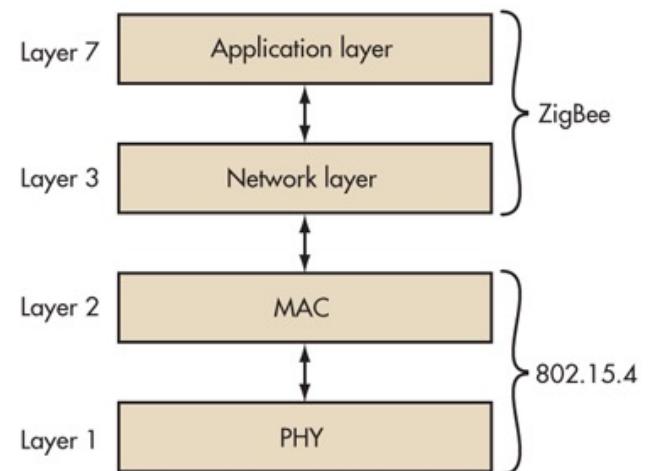
Geoff Merrett
ELEC3227/6255: Networks

Outline

- Introduction
- The IEEE 802.15.4 PHYsical layer
- The IEEE 802.15.4 DLL/MAC layer

Introduction

- Standard for low-data-rate WPANs (>700 pgs)
 - <https://ieeexplore.ieee.org/document/7460875>
- 802.15 standard: only PHY + DLL/MAC
- Numerous revisions
 - 802.15.4a/b
 - 802.15.4c for China
 - 802.15.4d for Japan
 - 802.15.4e for industrial applications
 - 802.15.4f for active (battery powered) radio-frequency identification (RFID)
 - 802.15.4g for smart utility networks (SUNs) for monitoring the Smart Grid



Introduction

*“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, and a reasonable battery life**, while maintaining a **simple and flexible protocol**.”*

802.15.4 Frame Structure

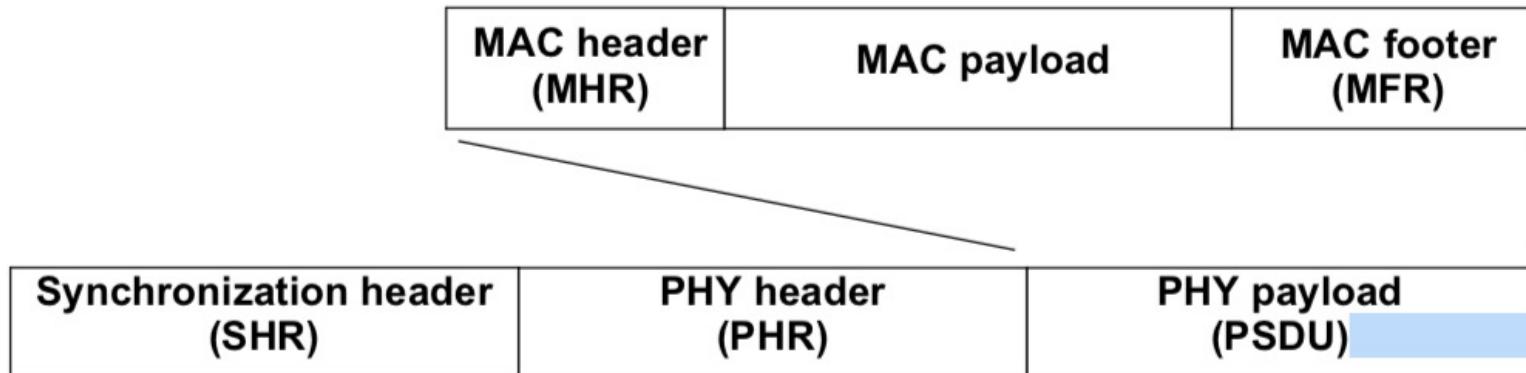


Figure 5-9—Schematic view of the PPDU

- **PPDU:** PHY Protocol Data Unit: the data transmitted/received on the channel
- **PSDU:** PHY Service Data Unit: the PHY payload
- **MPDU:** MAC Protocol Data Unit: the entire MAC frame, i.e. same as PSDU
- **MSDU:** MAC Service Data Unit: the MAC payload (i.e. the NPDU, etc)

Physical Layer

IEEE 802.15.4 Physical Layer

- Provides the following features:
 - Activation and deactivation of the radio transceiver
 - Channel Selection
 - Transmitting and Receiving data
 - Energy detection (ED)
 - A measure of the received signal power within the bandwidth of the selected channel, averaged over 8 symbol periods. No attempt is made to decode the data on the channel.
 - Link Quality Indication (LQI)
 - A measure of the signal strength or quality of a received packet
 - Clear Channel Assessment (CCA), at least one of the following
 - Energy above a threshold
 - Carrier sense
 - Carrier sense + energy above threshold
 - ALOHA (i.e. carrier sense off)



The UK Frequency Allocations

Short Range Devices (SRDs) Shared Allocations Acronyms

A - Alarms	MDA - Movement Detection or Alert
CA - Cordless Audio	NS - Non-Specified including Telemetry and Telecommand
D - Dataways	RFID - Radio Frequency ID
DAV - Detection of Avalanche Victims	RW - Radio Waves
GP - General Purpose SRDs	RTT - Road Transport and Traffic Telematics
HA - Hearing Aids	RTTC - Telemetry and Telecommand Commercial
IA - Industrial Application	TTC - Telemetry and Telecommand General
IP - Industrial Process	VHF - Very High Frequency
LAN - Local Area Network	WF - Wireless Gateways
MB - Medical and Biological	VD - Video Distribution
MC - Model Control	ULPAMI - Ultra-low Power Active Medical Implants
MD - Metal Detectors	WA - Wireless Audio
	WVC - Wireless Video Cameras

Radio Service Legend

Civil and Military Use
Civil Use
Military Use
Radio Astronomy
Aeronautical Radionavigation
Earth Exploration - Satellite
Amateur
Aeronautical Mobile
Maritime Radionavigation
Radio Navigation
Meteorological Aids
Broadcasting
Fixed
Fixed Satellite Service
Amateur - Satellite
Inter - Satellite
Mobile Satellite
Land Mobile
Radio Location
Space Research
Space Operation
Mobile
Standard Frequency and Time Signal
Standard Frequency and Time Signal Satellite
Meteorological Satellite
Radionavigation Satellite

Notes

UK ISM applications are designated for use within this band

UHFs include bandings S and L

SHFs include bandings S, C, X, Ku, K, Ka and R

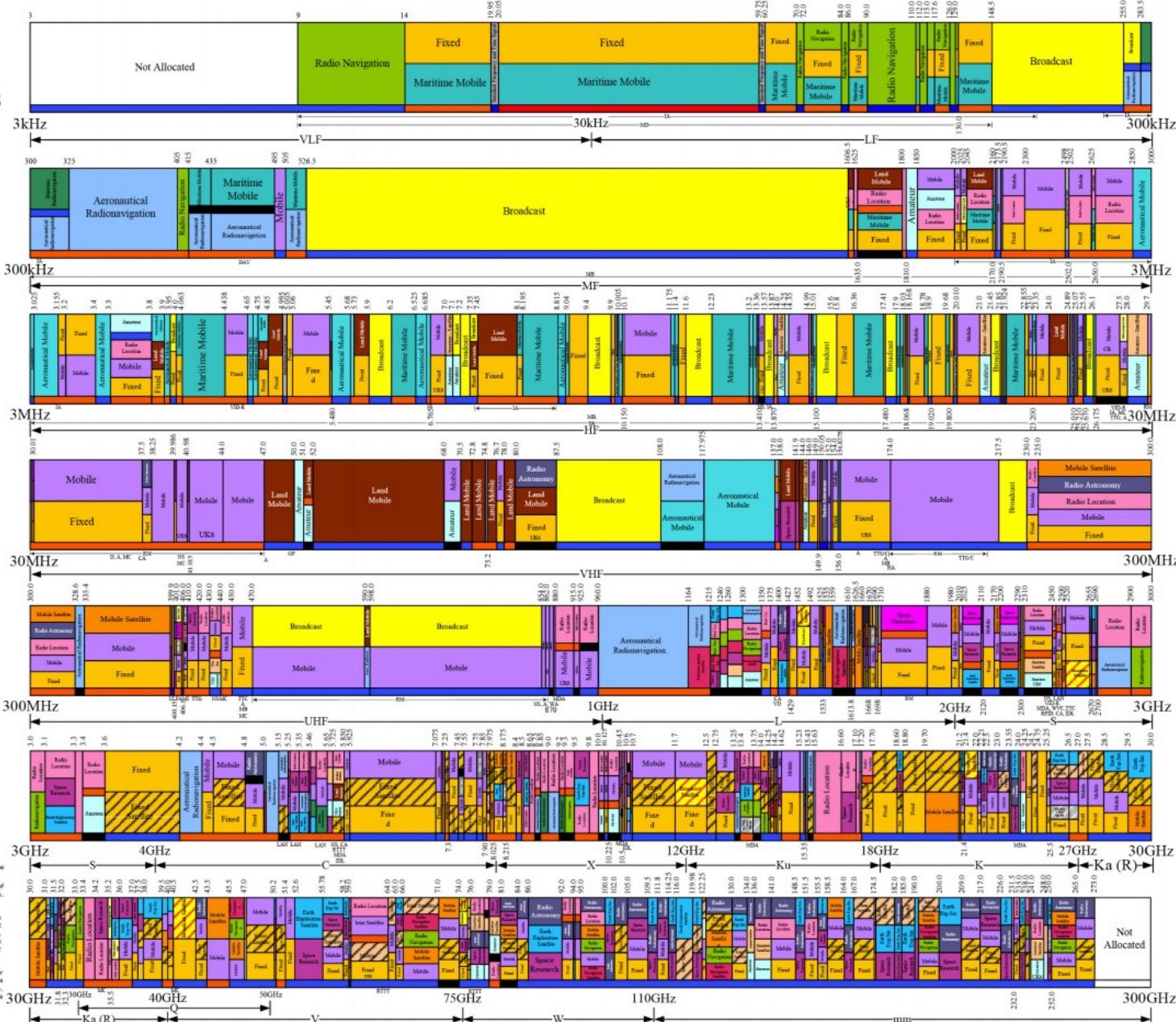
EHF's include bandings Ka, R, Q, V, W and millimeter (mm)

This chart does not differentiate between primary and secondary allocations. Details may be found in the UK FAT.

Frequencies for distress and safety, search and rescue and emergencies and the protection of frequencies for Radioastronomy are protected bands and should be avoided wherever possible. Details may be found in the UK FAT Annex H and D.

The authoritative document for spectrum allocations for the UK is the UK Frequency Allocation Table (UK FAT), published by Ofcom (www.ofcom.org.uk). This Frequency Allocation Chart is based on the latest version of the UK FAT, which will be the latest version of the table published by the Ofcom in 2007. UK spectrum allocations may change over time in accordance with decisions of the ITU, CEPT, European Commission, the UK Government or Ofcom.

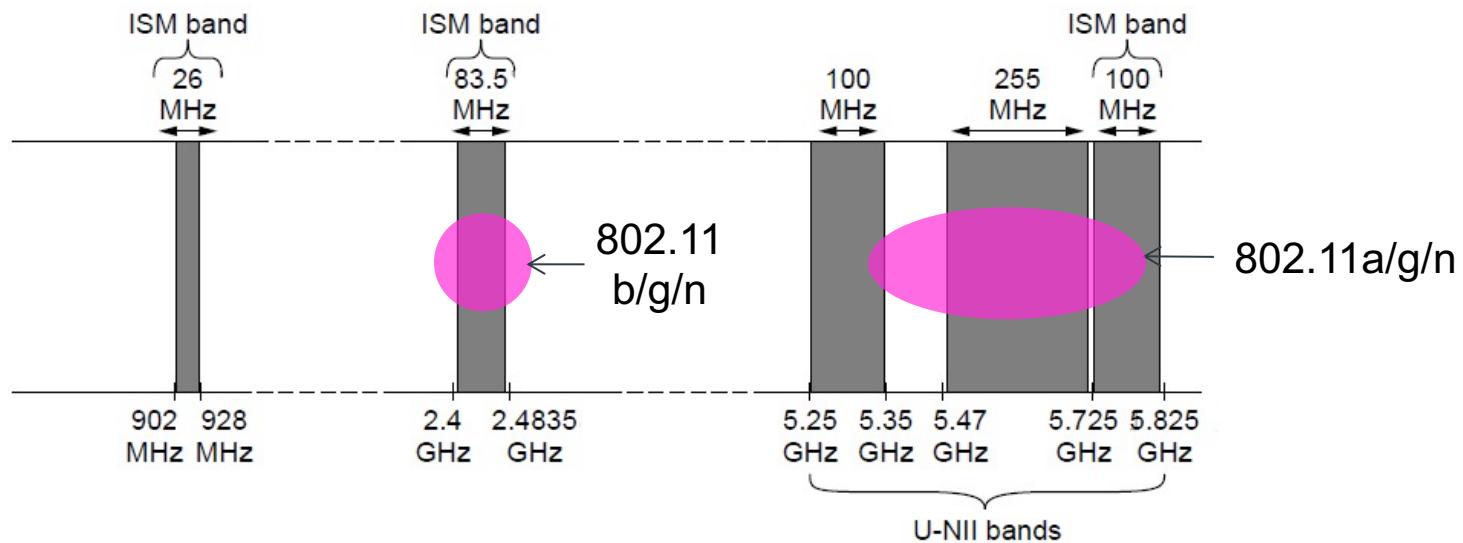
The Allocations table does not necessarily imply that the frequencies indicated are available for the use of particular services. It is the responsibility of the operator to check the relevant website which shows the frequencies for particular licence classes or for licence-exempt use. Ofcom also publishes the UK Spectrum Strategy, which contains guidance on future use on the spectrum in the UK.



To manage interference, spectrum is carefully divided, and its use regulated and licensed, e.g., sold at auction.

Electromagnetic Spectrum

- Fortunately, there are also unlicensed (“ISM”) bands:
 - Free for use at low power; devices manage interference
 - Widely used for networking; WiFi, Bluetooth, Zigbee, etc.



- Note, some of those shown above are not for the UK (e.g. 868 instead of 915 MHz)
- These are unlicensed, not unregulated...

IEEE 802.15.4 Physical Layer

- Originally supported frequency bands:
 - 868 MHz (Europe) @ 20 kbps, 1 channel, BPSK;
 - 915 MHz (North America) @ 40 kbps, 10 channels, BPSK;
 - 2.4 GHz (worldwide) @ 250 kbps, 16 channels, O-QPSK + DSSS
- However, standard has been significantly extended, to support other regions (e.g. China, Japan), frequency bands, encoding and modulation schemes, UWB, etc – now supporting data rates of up to 1 Mbps.

PHY Format

12.1 PPDU format

The PPDU shall be formatted as illustrated in Figure 12-1.



Figure 12-1—Format of the PPDU

- The PHR indicates the length of the PHY payload (i.e. the PSDU), which can be 0-127 octets

12.1.1 SHR field format

The SHR field shall be formatted as illustrated in Figure 12-2.

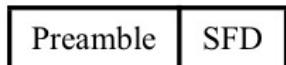


Figure 12-2—Format of the SHR

- Preamble = 32 bits (4 octets, 8 symbols)
- SFD indicates the end of the preamble, and is 11100101_2

Link/MAC Layer

IEEE 802.15.4 DLL/MAC Layer

- Provides the following features:
 - Association and disassociation
 - Beacon management
 - GTS management
 - Channel Access
 - Acknowledged frame delivery
 - Frame validation

Topologies

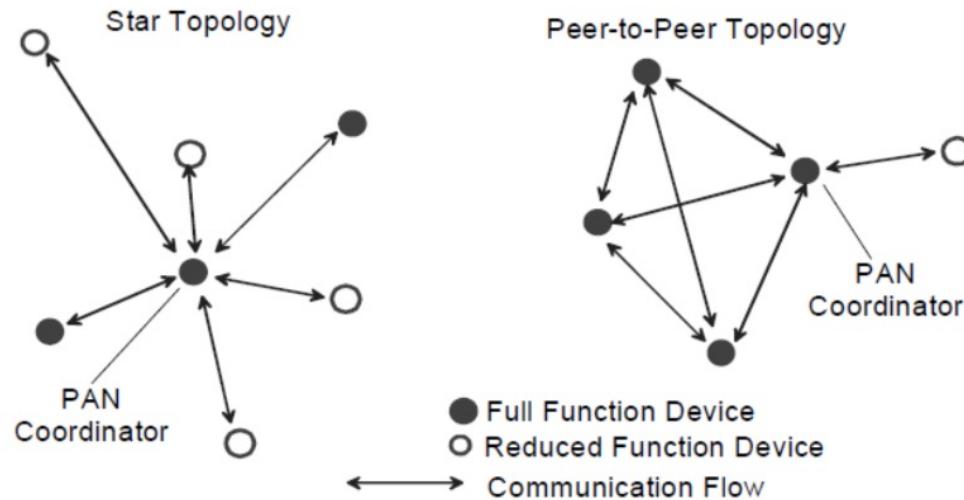


Figure 5-1—Star and peer-to-peer topology examples

- **FFD: Full-Function Device**, a “device capable of serving as a personal area network (PAN) coordinator or a coordinator”
- **RFD: Reduced-Function Device**, “intended for applications that are extremely simple, such as a light switch or PIR sensor; it does not need to send large amounts of data and only associates with a single FFD at a time. Consequently, can be implemented using minimal resources/memory capacity”¹⁴

Beacons

- IEEE 802.15.4 supports *beacon enabled* and *non-beacon enabled* models
- Beacons are used to:
 - Synchronise devices
 - Identify the PAN
 - Delimit superframes and describe structure (including GTS)
 - Synchronises slotted channel access
- In *non-beacon enabled* networks, devices have to request a beacon from the PAN coordinator (using an *active scan*) in order to identify the PAN and associate with it

PAN Formation and Device Discovery

- A FFD can start a PAN by performing an ED scan and active scan (to identify any existing PANs), and then selecting a unique PAN ID.
- The PAN coordinator indicates its presence to other devices by transmitting Beacon frames; devices can use this to discover the PAN using a passive scan.

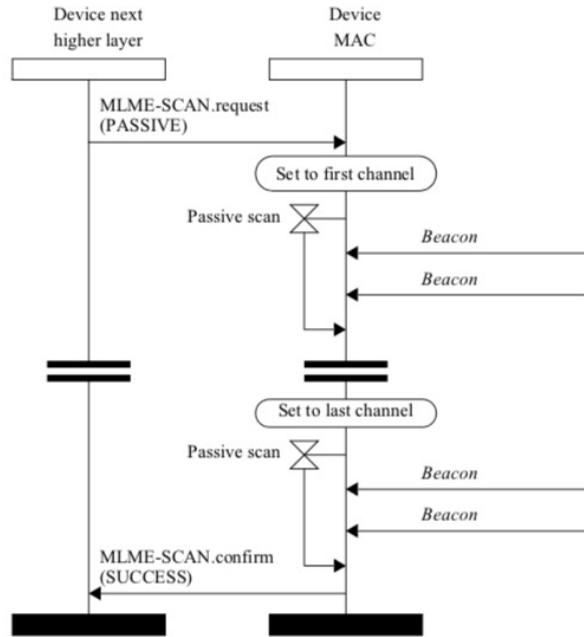


Figure 6-15—Passive scan message sequence chart

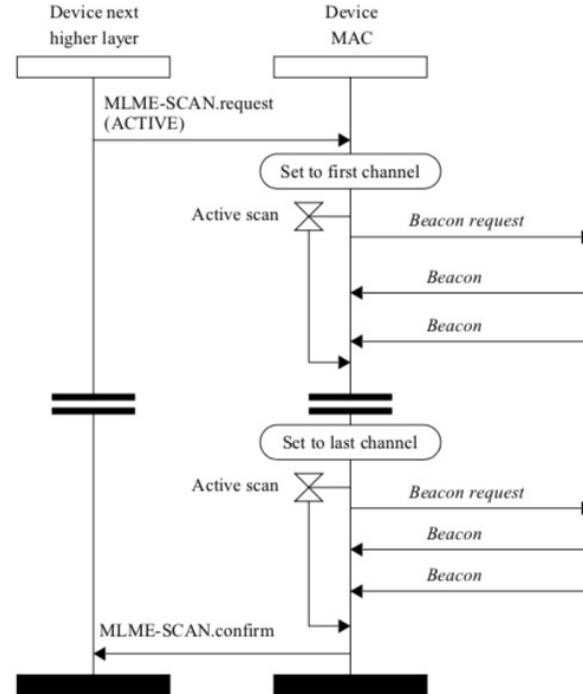


Figure 6-14—Active scan message sequence chart

Superframe Structure

- Active/Inactive Periods

Inactive period trades latency for energy efficiency

SD = Superframe Duration

BI = Beacon Interval

- Guaranteed Timeslots (GTS)

A Contention Free Period (CFP) suited for low-latency applications, or those requiring specific data bandwidth. CSMA not used.

The PAN coordinator can allocate up to 7 GTSs; however, a Contention Access Period (CAP) always remains.

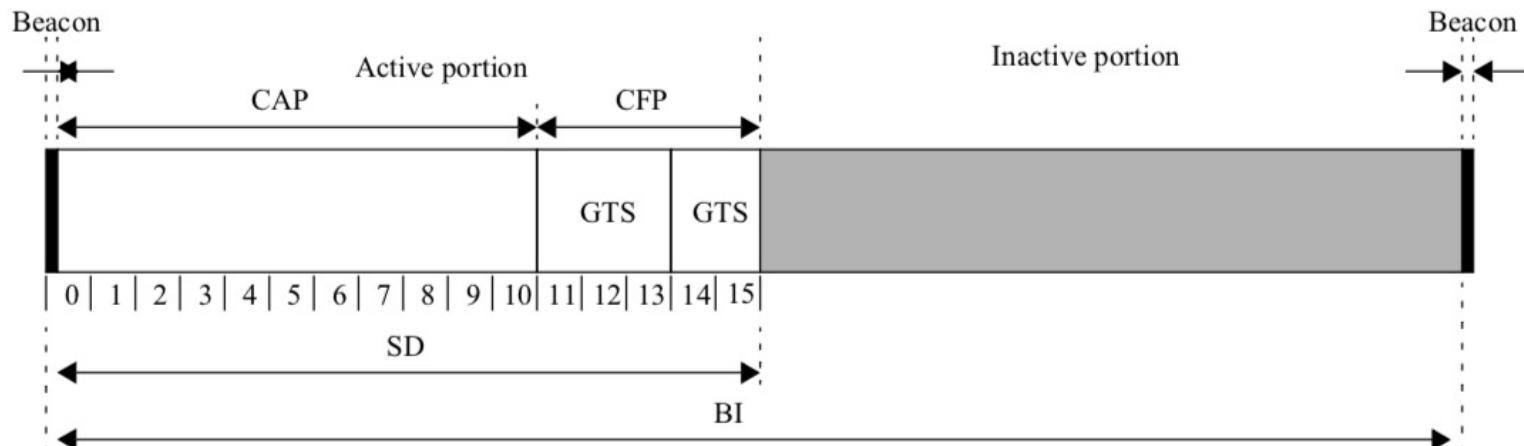
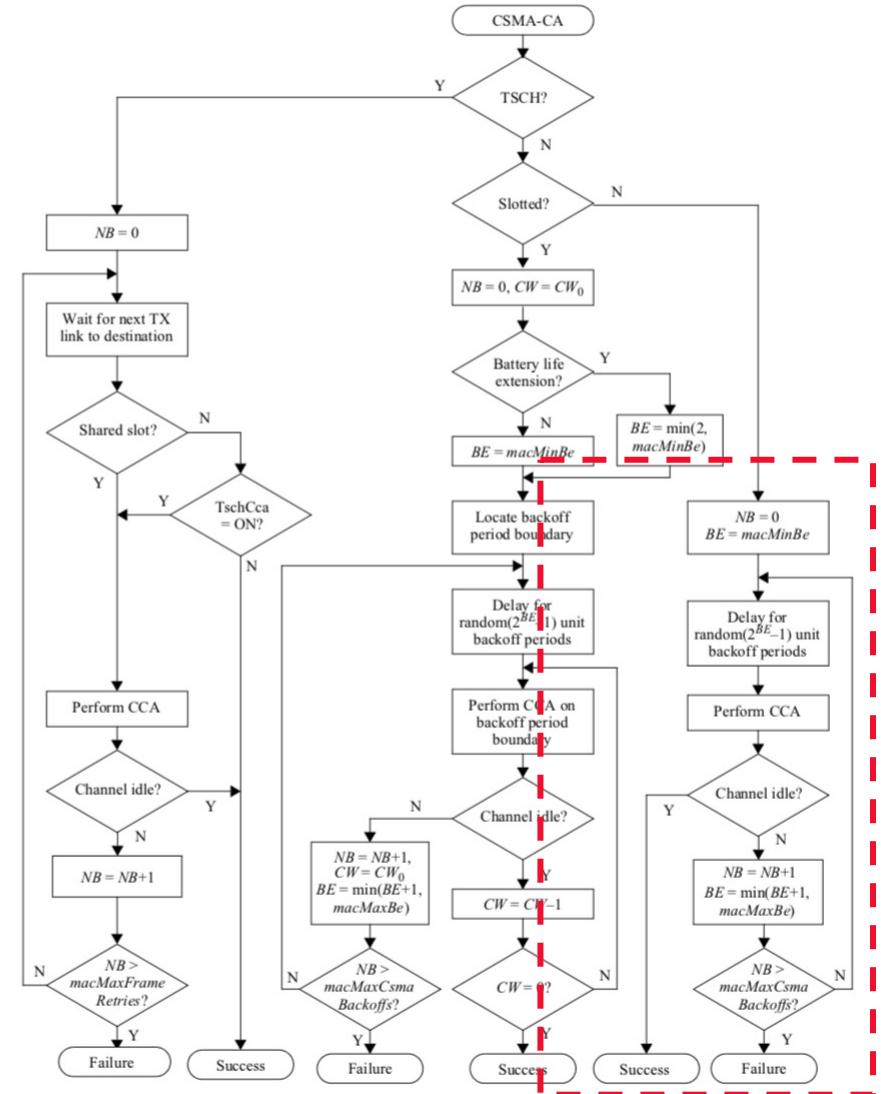


Figure 6-1—An example of the superframe structure

CSMA-CA

- Backs off for a period of $\text{random}(2^{BE} - 1) * aUnitBackoffPeriod$
- Slotted CSMA-CA (Beacon-enabled)
 - Backoff aligned with superframe slots
- Unslotted CSMA-CA
 - Backoff periods are not slotted
- **NB**: number of times backed-off; stops when reaches predefined value
- **BE**: backoff exponent; increments by 1 each time
- **CW**: contention window length, defines how long the channel needs to be clear before transmitting



Acknowledgements

- The layer supports
 - **Unacknowledged:** an acknowledgement is not requested from the receiver, and the sender assumes that it was successfully received.

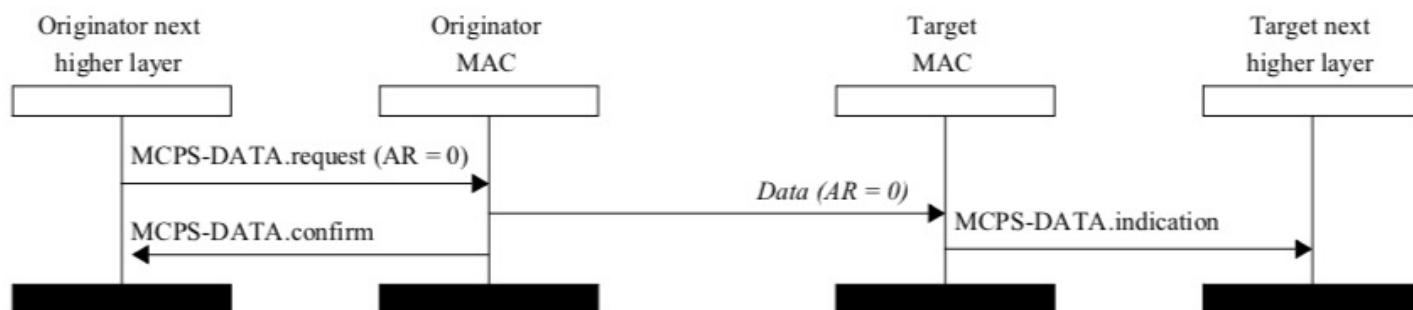


Figure 6-34—Successful data transmission without an acknowledgment

Acknowledgements

- The layer supports
 - **Acknowledged:** if the AR (acknowledgement request) field is set, an acknowledgement is requested from the receiver.

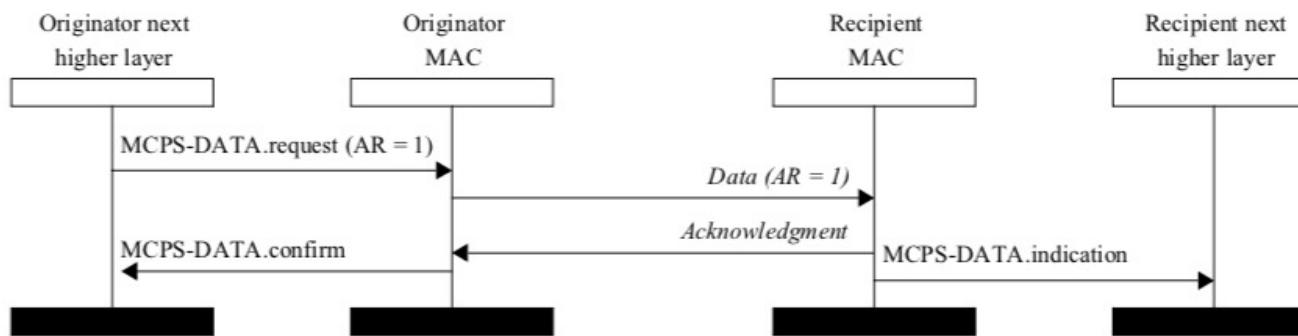


Figure 6-35—Successful data transmission with an acknowledgment

- If an Ack frame is not received within the expected time or the Ack frame that is received contains a DSN that was not the same as the original transmission, the device shall conclude that the single transmission attempt has failed.

MAC Frame Format

Octets: 1/2	0/1	0/2	0/2/8	0/2	0/2/8	variable	variable	variable	2/4
Frame Control	Sequence Number	Destination PAN ID	Destination Address	Source PAN ID	Source Address	Auxiliary Security Header	IE	Frame Payload	FCS
MHR									
MAC Payload						Header IEs	Payload IEs	MFR	

Figure 7-1—General MAC frame format

Frame Control Field

Bits: 0–2	3	4	5	6	7	8	9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Sequence Number Suppression	IE Present	Destination Addressing Mode	Frame Version	Source Addressing Mode

Figure 7-2—Format of the Frame Control field

Frame type value b2 b1 b0	Description
000	Beacon
001	Data
010	Acknowledgment
011	MAC command
100	Reserved
101	Multipurpose
110	Fragment or Frak ^a
111	Extended

MAC Frame Format

Octets: 1/2	0/1	0/2	0/2/8	0/2	0/2/8	variable	variable	variable	2/4
Frame Control	Sequence Number	Destination PAN ID	Destination Address	Source PAN ID	Source Address	Auxiliary Security Header	IE		FCS
	Addressing fields						Header IEs	Payload IEs	
MHR						MAC Payload		MFR	

Figure 7-1—General MAC frame format

Addressing

- All devices have a unique 64-bit *extended address* (an extended universal identifier, EUI-64), assigned by a regulatory authority (e.g. the IEEE)
- After a device has associated with a PAN, and been allocated a *short address*, (unique only in the PAN) it uses this wherever possible.

MAC Frame Format

Octets: 1/2	0/1	0/2	0/2/8	0/2	0/2/8	variable	variable	variable	2/4
Frame Control	Sequence Number	Destination PAN ID	Destination Address	Source PAN ID	Source Address	Auxiliary Security Header	IE	Frame Payload	FCS
MHR									
MAC Payload						Header IEs	Payload IEs	MFR	

Figure 7-1—General MAC frame format

Checksum (FCS Field)

- One of the following is calculated over the MHR and MAC payload parts of the frame:
- 16-bit ITU-T CRC
 - $G_{16}(x) = x^{16} + x^{12} + x^5 + 1$
- 32-bit CRC equivalent to ANSI X3.66-1979
 - $G_{32}(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$



Questions?