VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF TELECOMMUNICATIONS

Telecommunication Networks

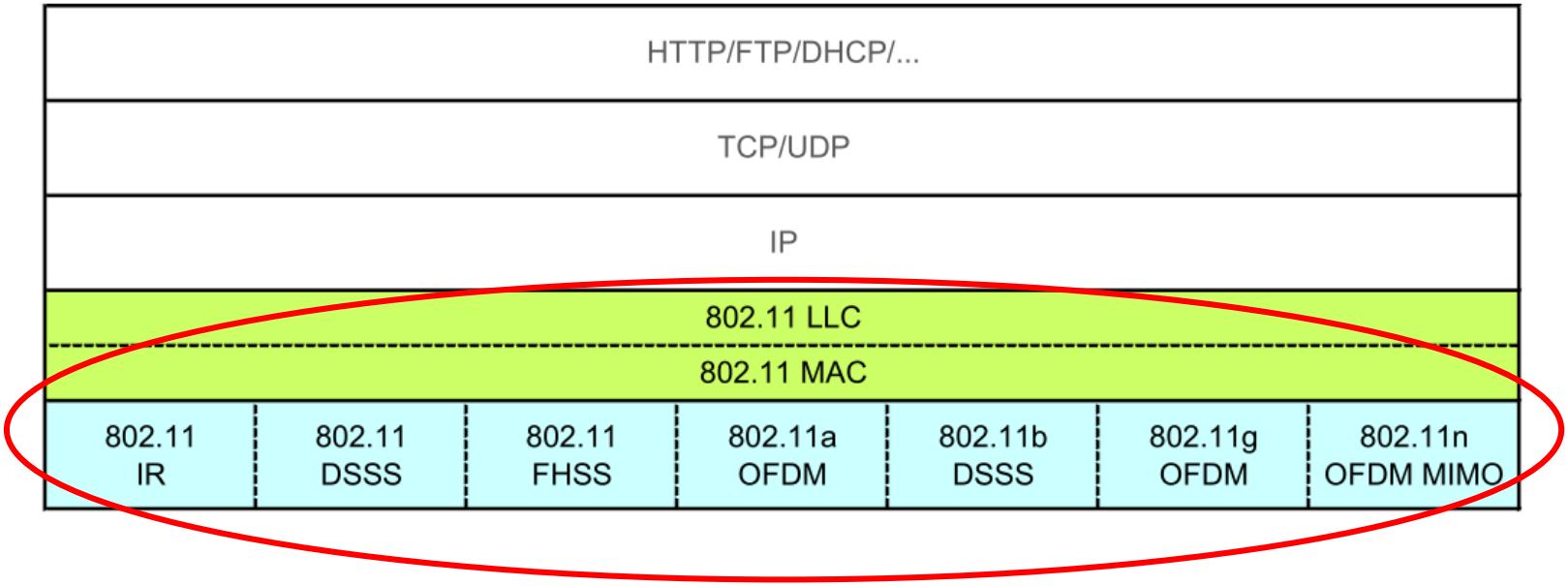
Wireless Access Networks

Libor Michalek

WLAN Technology

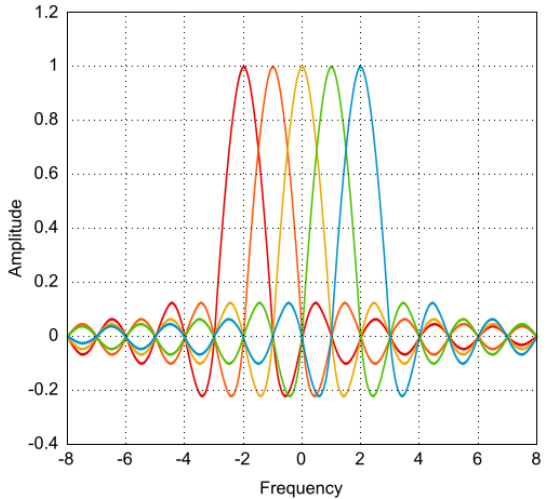
source: Wi-Fi Alliance

- known as WiFi, or IEEE 802.11
- standard defines:
  - the physical layer (PHY)
  - the data link layer - comprise of two sub-layers:



WLAN Physical Layer

- the physical layer defines the spectrum technique, modulation a frequency band
- **Spectrum Techniques:**
  - **FHSS** (Frequency Hopping Spread Spectrum)
    - 79 channels, each 1MHz
    - 400 ms is time fo transmitting
    - lower bitrates than DSSS, obsolote – not used
  - **DSSS** (Direct Sequence Spread Spectrum)
    - data signal is combined with a high data rate bit sequence with use of XOR operation
    - the bitrate is spreaded → chiprate
  - **OFDM** (Orthogonal Frequency Division Multiplexing)
    - large number of closely spaced orthogonal sub-carrier signals are used
    - robust against fading and multipath propagation



WLAN Physical Layer

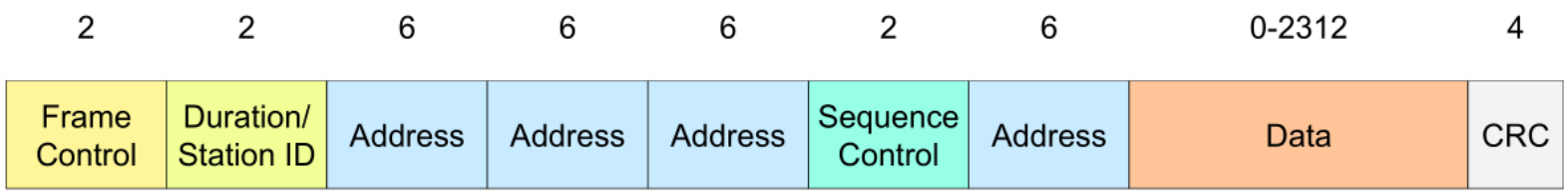
Ozn.	Kmitočtové pásmo	Maximální vyzářený výkon	Maximální spektrální hustota e.i.r.p.	Další podmínky	Harmonizovaná norma (ČSN ETSI EN)[2])
a	2400,0–2483,5 MHz	100 mW e.i.r.p.	10 mW/1 MHz	systémy s technikou DSSS[4]) nebo OFDM[5])	300 328[6])
			100 mW/100 kHz	systémy s technikou FHSS[7])	
b1	5150–5250 MHz	200 mW e.i.r.p.[8])	10 mW/MHz	pouze pro použití uvnitř budovy[9])	301 893[10])
b2	5250–5350 MHz				
b3	5470–5725 MHz	1 W e.i.r.p.[8])	50 mW/MHz	—	
c	17,1–17,3 GHz	100 mW e.i.r.p.[8])	—	—	dosud nestanovena[11])
d1	57–66 GHz	40 dBm e.i.r.p.[8])	13 dBm/MHz	Pevné venkovní instalace[12]) jsou vyloučeny	302 567[13])
d2	57–71 GHz	40 dBm e.i.r.p.[8])	23 dBm/MHz	Pevné venkovní instalace[12]) jsou vyloučeny	dosud nestanovena[11])
d3	57–71 GHz	40 dBm e.i.r.p.[8])	23 dBm/MHz, výkon přivedený do antény je max. 27 dBm	Včetně pevných venkovních instalací[12])	
d4	57–71 GHz	55 dBm e.i.r.p.[8])	38 dBm/MHz, zisk antény je min. 30 dBi	Pouze pevné venkovní instalace[12])	
d5	57–64 GHz	55 dBm e.i.r.p.	výkon přivedený do antény je max. 10 dBm, zisk antény je min. 30 dBi	Pevné vysokorychlostní spoje typu bod-bod; možnost vzájemné kombinace TDD a FDD	302 217-3[14])
d6	64–66 GHz				

In Czech Republic, **operation of any WLAN device must fulfil General License requirements** released by ČTÚ, **„Všeobecné oprávnění č. VO-R/12/12.2019-10“**
https://www.ctu.cz/sites/default/files/obsah/ctu/vseobecne-opravneni-c.vo-r/12/12.2019-10/obrazky/vo-r12-122019-10.pdf

8) Při použití regulace výkonu se uvedené hodnoty vztahují ke střednímu ekvivalentnímu izotropicky vyzářenému výkonu (mean, tj. střední e.i.r.p.), tj. výkonu po dobu vysílání, který odpovídá nejvyššímu výkonu, resp. ke střední spektrální hustotě, tj. střednímu e.i.r.p. na 1 MHz.

WLAN Link Layer

- **defines structure of frame, access method, multiplexing technique, error protection and ciphering**
- two sublayers are defined:
  - **LLC** (Logical Link Control)
  - **MAC** (Media Access Control)
- **MAC layer**
  - defines access method, frame structure and protection
- 3 categories of frames are defined on MAC sublayer
  - **management** – function of WLAN (Association Request, Beacon, Association Response)
  - **control** – function of access method (RTS, CTS, ACK)
  - **data** – transmission of frames

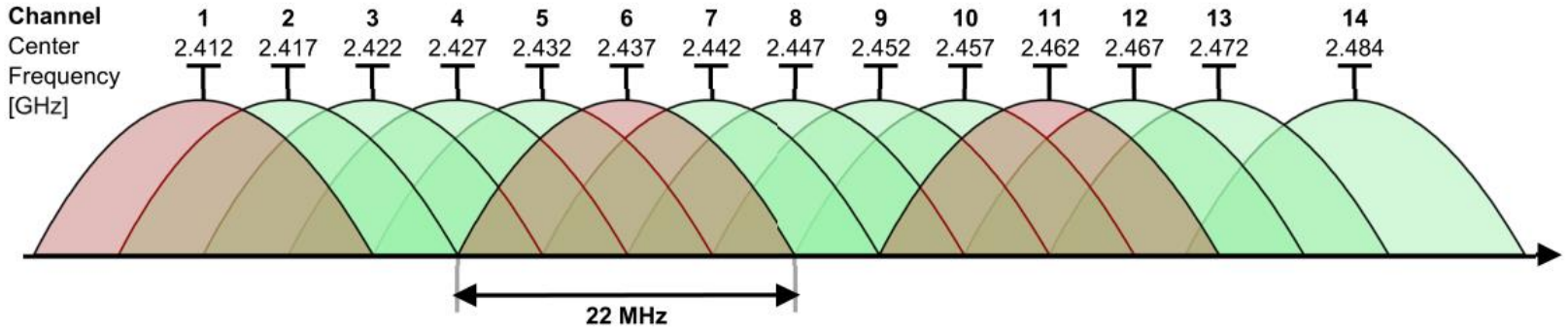


IEEE 802.11 data frame

IEEE 802.11 family of specifications

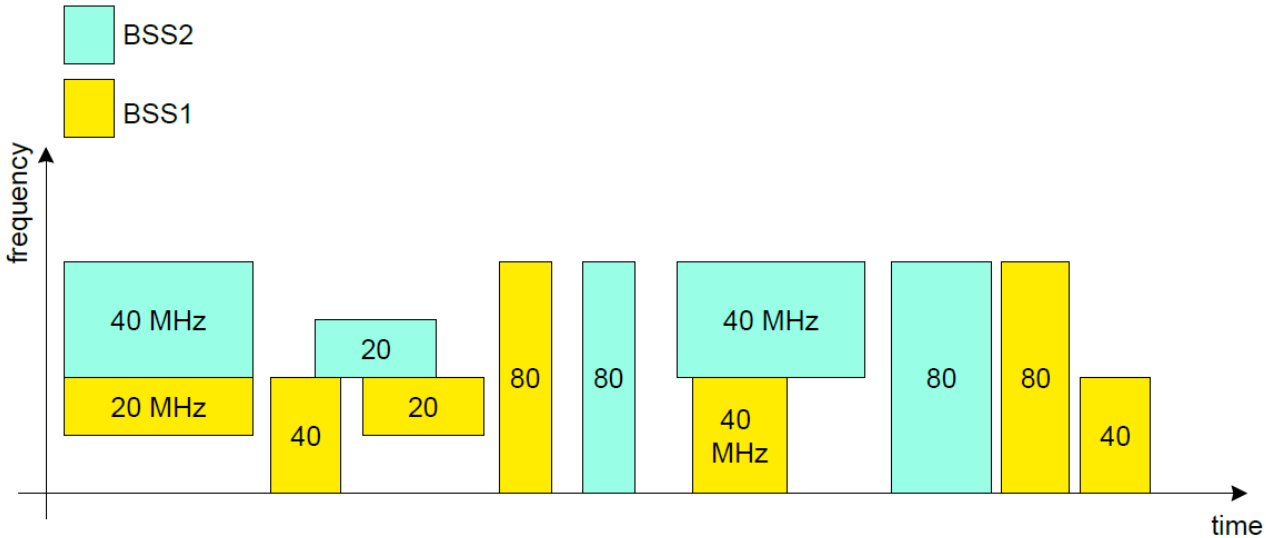
source: Wi-Fi Alliance

- **802.11**
  - 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS), obsolete
- **802.11a (WiFi 2)**
  - 5150-5725 MHz, 20 MHz channel, no MIMO
- **802.11b (WiFi 1)**
  - **ISM** band 2.4 GHz,
  - up to 11 Mb/s, DSSS on physical layer, 14 channels defined
  - 5 MHz span between each channel
  - 22 MHz bandwidth of each channel → overlap of adjacent channels
  - maximum EIRP = 100 mW!



IEEE 802.11 family of specifications

- **802.11g (WiFi 3)**
  - uses OFDM, back compatibility to 802.11b, up to 54 Mb/s
- **802.11n (WiFi 4)**
  - builds upon previous 802.11 standards by adding *MIMO (multiple-input multiple-output)*
  - MIMO is a method for multiplying the capacity of a radio link using multiple transmit and receive antennas to exploit multipath propagation
- **802.11ac (WiFi 5)**
  - reservation of mulitple 20 MHz channels
  - primary 20 MHz channel is always choosen (transmitting of **Beacon**)
  - total bandwidth is adaptivelly changed based on actual level in interference
  - bandwidth up to 160 MHz
  - up to 256-QAM



IEEE 802.11 family of specifications

- **802.11ad**
  - as **WiGig,** in 2008 **TGad** workgroup under IEEE established
  - operation in 57 – 66 GHz, 2160 MHz channel
  - up to 7 Gb/s
  - successor will be *802.11ay*
- **802.11ax (WiFi 6)** *(High-Efficiency Wireless)*
  - 2,4 and 5 GHz
  - lower subcarrier spacing
  - 600 Mbps (80 MHz)
  - 9600 Mbps (160 MHz, 8x8 MIMO)
  - 1024-QAM (25% increase to 256QAM)
  - fully approved in Q3/2019

	802.11a/g	802.11n/ac	802.11ax
Sub-carrier spacing	20MHz/64 = 312.5KHz	20MHz/64 = 312.5KHz	20MHz/256 = 78.125KHz
Subcarriers	48	52	234
Efficiency	75%	81%	91%

- **802.11ah**
  - for IoT and M2M support
  - 863 – 868 MHz
  - 1 MHz or 2 MHz channel bandwidth
  - up to 8 Mbps, commonly ~ 1Mbps

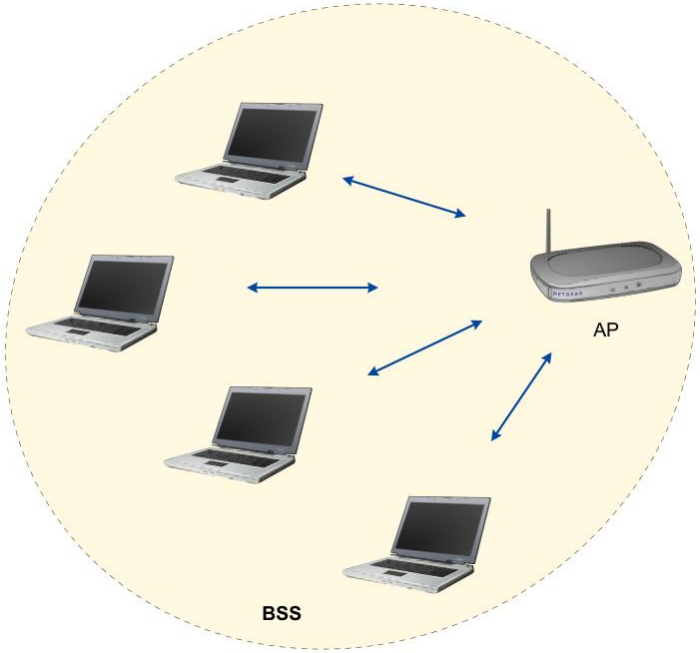
Comparison of 802.11 specifications

	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Year Ratified	1997	1999	1999	2003	2009	2014	2019 (Expected)
Operating Band	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz
Channel BW	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Peak PHY Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	9.6 Gbps
Link Spectral Efficiency	0.1 bps/Hz	0.55 bps/Hz	2.7 bps/Hz	2.7 bps/Hz	15 bps/Hz	42.5 bps/Hz	62.5 bps/Hz
Max SU Streams	1	1	1	1	4	8	8
Max MU Streams	NA	NA	NA	NA	NA	4 (DL only)	8 (UL & DL)
Modulation	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM, OFDMA
Max Constellation / Code Rate	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Max # OFDM tones	NA	NA	64	64	128	512	2048
Subcarrier Spacing	NA	NA	312.5 kHz	312.5 kHz	312.5 kHz	312.5 kHz	78.125 kHz

WLAN operating modes

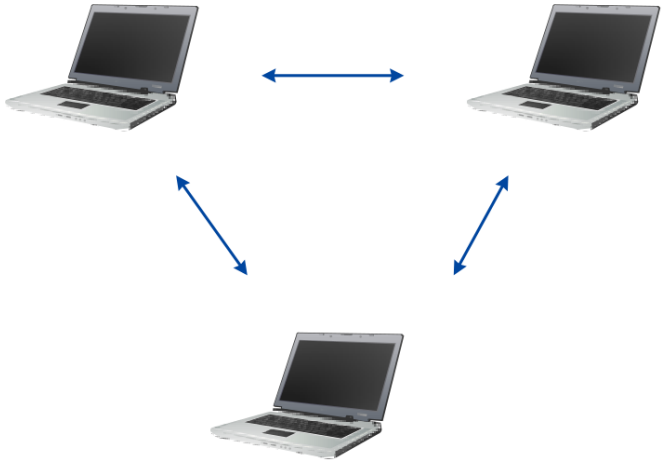
Infrastructure mode

- wireless clients are connected to an access point
- the set-up formed by the access point and the stations located within its coverage area are called the basic service set (BSS).



Ad hoc mode

- clients are connected to one another without any access point



WLAN Network Security

- **SSID blocking** vulnerable !
- **Filtering MAC addresses** vulnerable !
  - The configuration of access points generally allow them to keep a list of access permissions (called the ACL, for Access Control List) based on the MAC addresses of the devices authorised to connect to the wireless network
- **WEP - Wired Equivalent Privacy** vulnerable !
  - data frame encryption protocol that uses the symmetrical algorithm RC4 with 64-bit or 128-bit keys
  - obsolete, cracked
- **WPA - WPA - WiFi Protected Access** vulnerable !
  - relies on a strong encryption algorithm TKIP (Temporary Key Integrity Protocol)
  - TKIP generates keys randomly and can alter an encryption key several times a second, for greater security

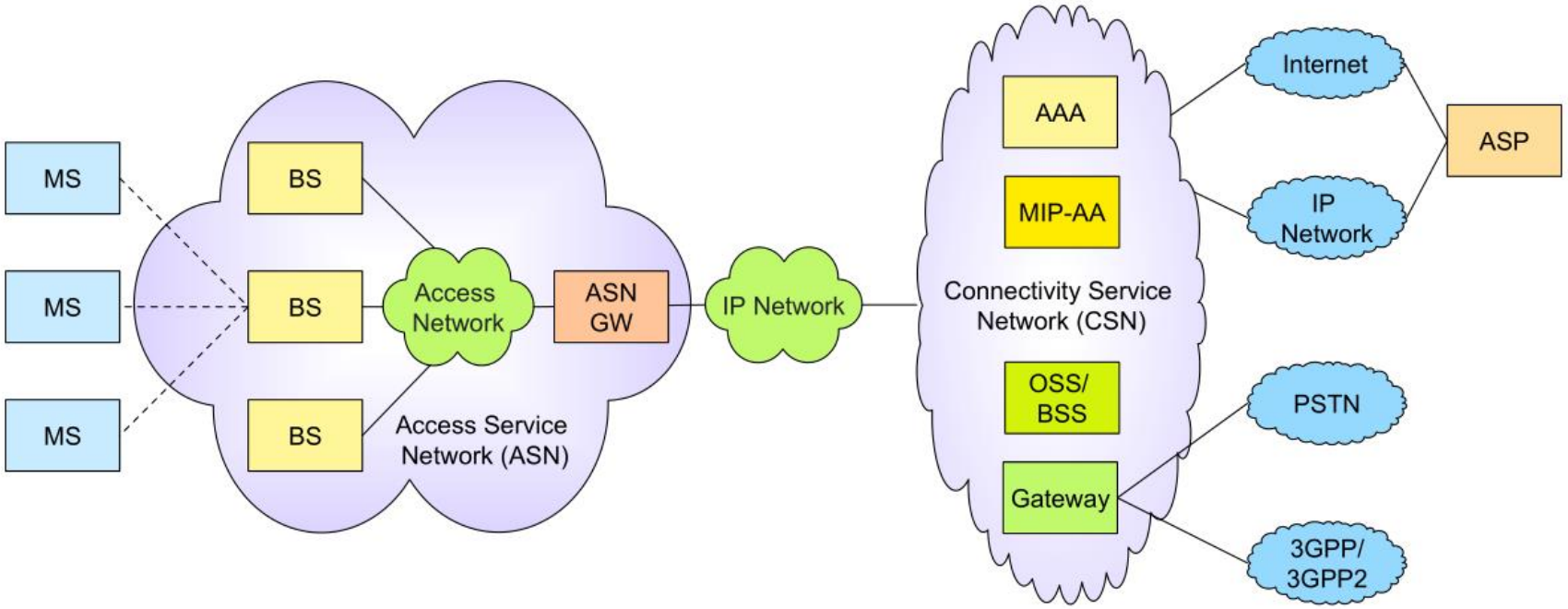
WLAN Network Security

- **802.11i / WPA2**
  - like WPA, it relies on the TKIP + AES (Advanced Encryption Standard), not RC-4
  - created by WiFi Alliance
  - use of a PSK (Pre-shared Key), which is stored at both the access point and the client devices
  - or use an authentication server, generally a RADIUS server (which stands for Remote Authentication Dial-in User Service)
- **WPA3**
  - introduced in 2018
  - 128-bit encryption in WPA3-Personal mode, 192-bit in WPA3-Enterprise
  - WPA3 replaces the Pre-Shared Key exchange with more secure initial key exchange - **Simultaneous Authentication of Equals** (SAE)
- **802.1x / EAP**
  - can authenticate (identify) a user who wants to access a network
  - this is done through the use of an authentication server
  - 802.1x is based on the EAP protocol (Extensible Authentication Protocol)
  - EAP protocol is used for transporting user identification information

WiMAX

- Worldwide Interoperability for Microwave Access
- ratified by the IEEE under the name IEEE 802.16
- last mile wireless broadband access as an alternative to cable and DSL
- the goal of WiMAX was to provide high-speed Internet access in a coverage range several kilometres in radius
- versions (since 2002):
  - **802.16** (2001) – 10-66 GHz, up to 134 Mbit/s, BPSK, QPSK
  - **802.16d** (2004) - 2-11 GHz; up to 75 Mbit/s, OFDMA
  - **802.16e** (2005) mobile WiMAX, 2-6 GHz; up to 128 Mbit/s at 120 km/h
  - **802.16m** (2009), so-called WIMAX 2.0, last variant, 0,45-3,6 GHz, up to 300 Mbit/s, use of MIMO, up to 64QAM
- unfortunately, technology failed to attract widespread support from equipment vendors and other wireless operators

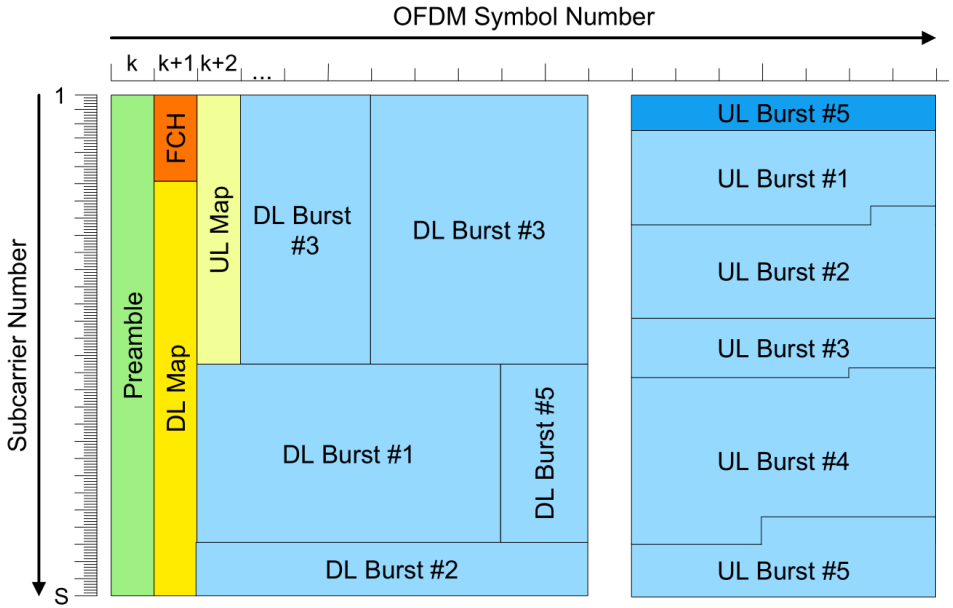
WIMAX Architecture



- **BS** (Base Station)
- **MS** (Mobile Station)
- **ASN** (Access Service Network)
- **CSN** (Connectivity Service Network)

WIMAX Physical Layer

- support of duplex modes:
  - FDD (Frequency Division Duplex)
  - TDD (Time Division Duplex)
- following frequency bands are used:
  - 450 - 470 MHz
  - 698 - 960 MHz
  - 1710 - 2025 MHz
  - 2110 - 2200 MHz
  - 2300 - 2400 MHz
  - 2500 - 2690 MHz
  - 3400 - 3600 MHz
- use od OFDM and MIMO
- use up to 64QAM



WIMAX time-frequency map

Bluetooth

- Wireless Personal Area Network Technology (WPAN)
- low-range wireless network technology used for linking devices to one another without a hard-wired connection
- do not need a direct line of sight to communicate
- he aim is to transmit voice or data between devices with low-cost radio circuits, over a range of about ten to just under a hundred metres, using very little power
- designed mainly for linking devices (such as printers, mobile phones, home appliances, wireless headsets, mouses, keyboards, etc.), computers, or PDAs to one another, without using a wired connection
- becoming more and more commonly used in mobile phones, allowing them to communicate with computers or PDAs

Bluetooth operational modes

a) master - slave

b) piconet

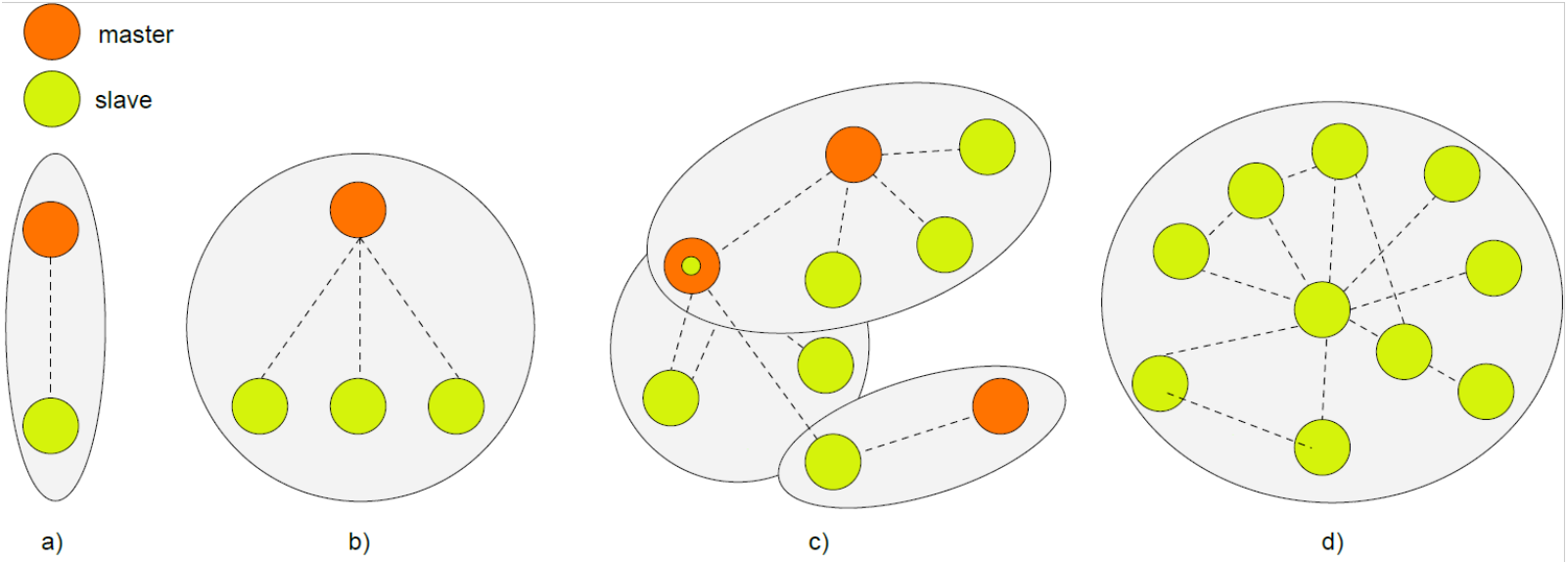
a master can be simultaneously connected to as many as 7 active slave devices, up to version 3

c) scatternet

scatternets can be formed when a member of one piconet (either the master or one of the slaves), up to version 3

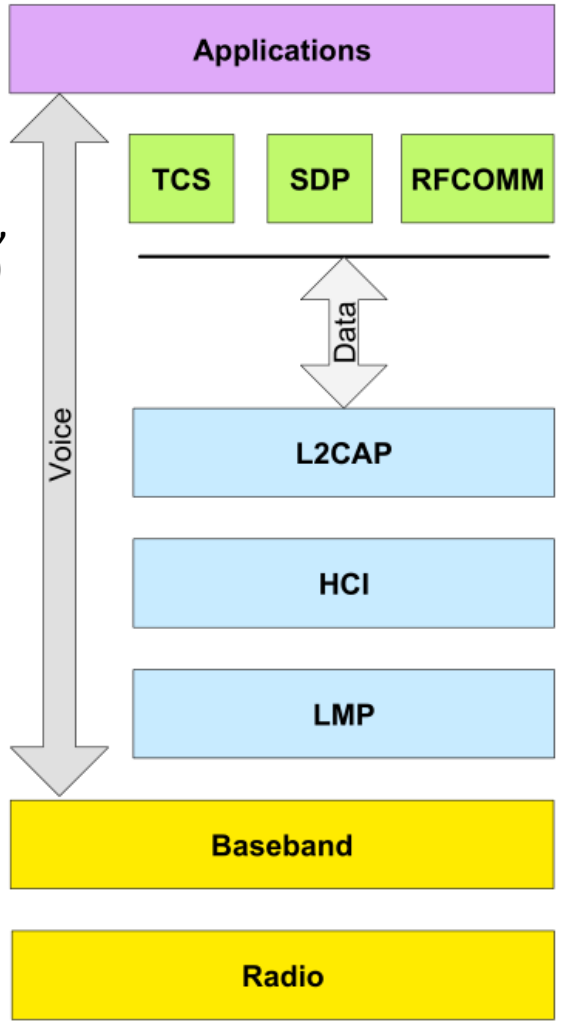
d) mesh

number of slaves is not limited, from version 4



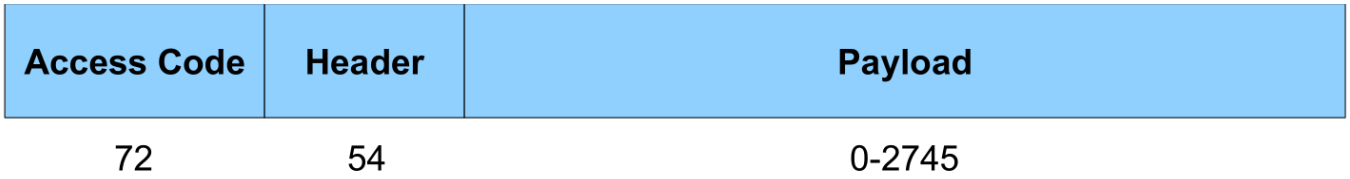
Bluetooth Protocol stack

- **Bluetooth radio**
  - 2,4 GHz frequency band with GFSK (Gaussian Frequency Shift Keying)
  - FHSS technique (Frequency-Hopping Spread Spectrum), which splits frequency band of 2.402-2.480 GHz into 79 channels (called hops) each 1MHz wide
  - 1600 hops per second in full-duplex mode
  - defines 3 classes of transmitters, whose range varies as a function of their radiating power
    - Class 1 – up to 100 mW
    - Class 2 – up to 2,5 mW
    - **Class 3 – up to 1 mW**
- **Bluetooth Baseband**
  - defines access mechanism for transmission medium, duplex method (TDD)
- **LMP (Link Manager Protocol)**
  - for procedures such as Inquiry, Paging and Pairing



Bluetooth Protocol stack

- **L2CAP (Logical Link Control and Adaptation Protocol)**
  - format of packet is defined



  - Access Code (72 bits) – for synchronization
  - Header (54 bits) – addressing, flow control, error protection
  - Payload (0-2745 bits)
- **RFCOMM (Radio Frequency Communication)**
  - emulating of RS-232 serial port
- **SDP (Service Discovery Protocol)**
  - for discovering the Bluetooth equipment and its services

Bluetooth Versions

	Version 1-3	Version 4	Version 5
Frequency [MHz]	2400-2483.5	2400-2483.5	2400-2483.5
Range [m]	100	100	200
Spectrum	FHSS	FHSS	FHSS
Throughput [Mb/s]	3	1	2
Latency [ms]	<100	<6	<3
Topology	piconet, scatternet	star-bus, mesh	star-bus, mesh
Max. number of slaves	7	unlimited	unlimited
Message size [B]	up to 358	31	255
Max. output power [mW]	100	100	100

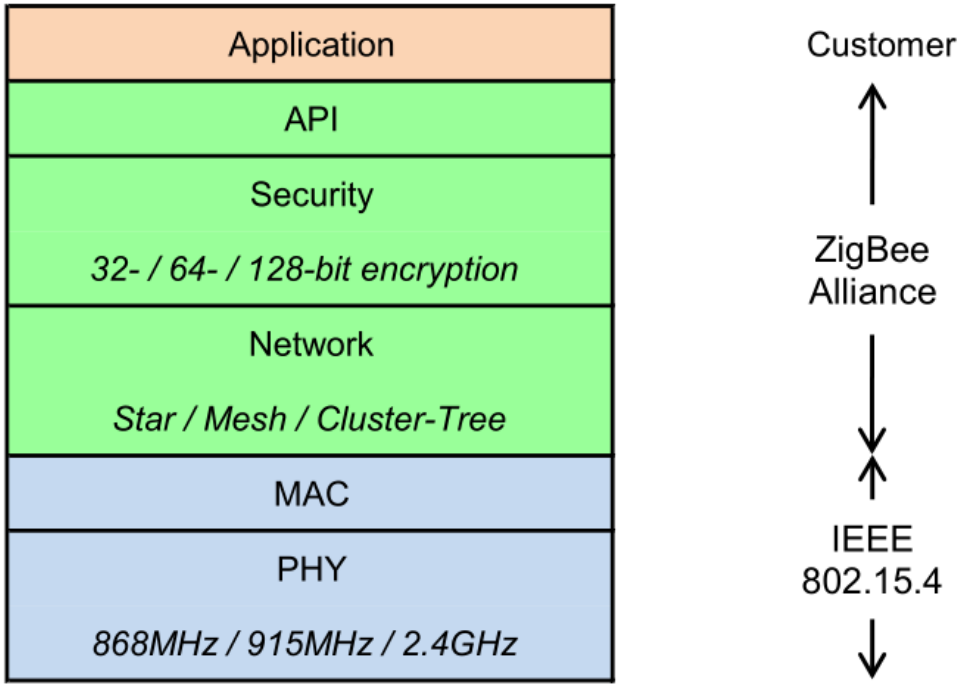
Zigbee

ZigBee Alliance

- specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard
- simpler and less expensive than other WPANs, such as Bluetooth
- Wireless monitoring, control of lights, security alarms, motion sensors, thermostats, pressure sensors, smoke detectors…
- Low power consumption
- Low cost
- Low offered message throughput
- Supports large network orders (<= 65k nodes)

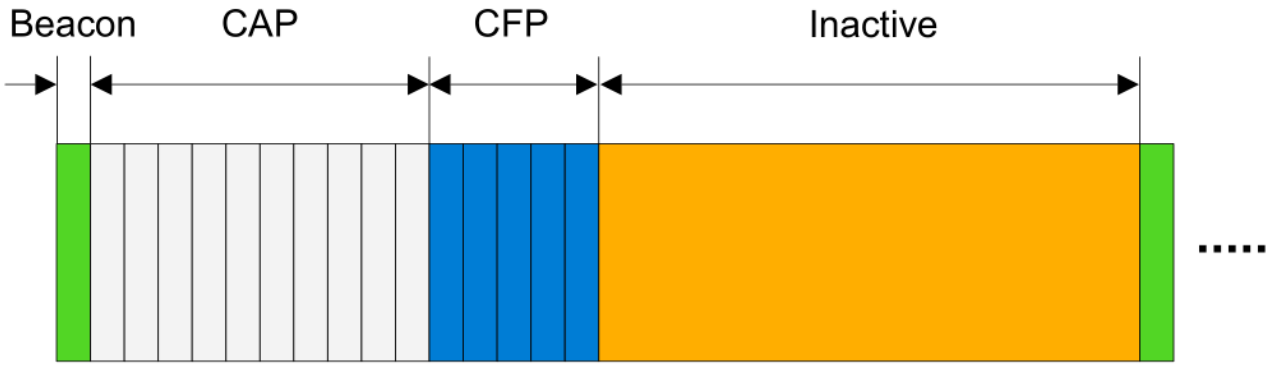
Zigbee Protocol Stack

- IEEE 802.15.4 defines **PHY and MAC layer**
- ZigBee Alliance defines **network and security layer**



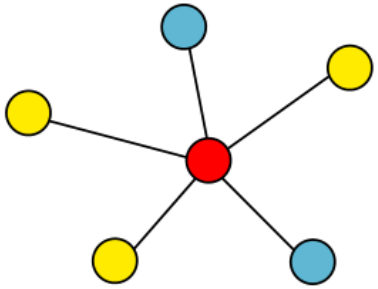
Zigbee physical layer

- **Physical Layer**
  - use of BPSK or QPSK, 20 kb/s
  - frequency band: **868 MHz**, 902-928 MHz, 2400 MHz
- **MAC layer**
  - synchronization, error protection, ciphering, management of frames
  - frames divides into
    - Beacon - transmitted by network coordinator, contains network information
    - CAP (Contention Access Period) - Access by any node using CSMA-CA
    - CFP (Contention Free Period) - Reserved for nodes requiring guaranteed bandwidth
    - Inactive – low power mode

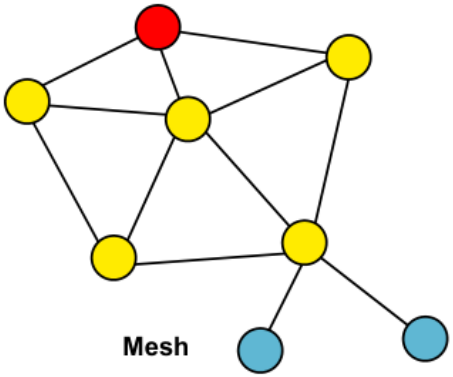


Zigbee Topology

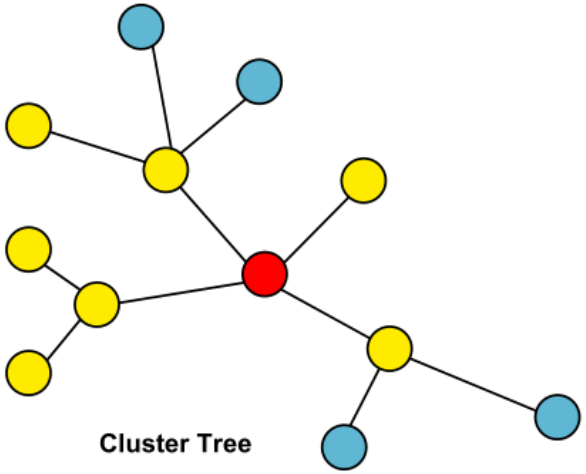
- support of star, tree and mesh topology
- **PAN coordinator** - responsible for initializing, maintaining, and controlling the network
- **FFD** - talks to any other device
- **RFD** - talks only to a network coordinator



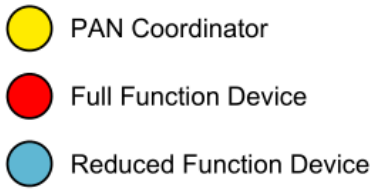
Star



Mesh

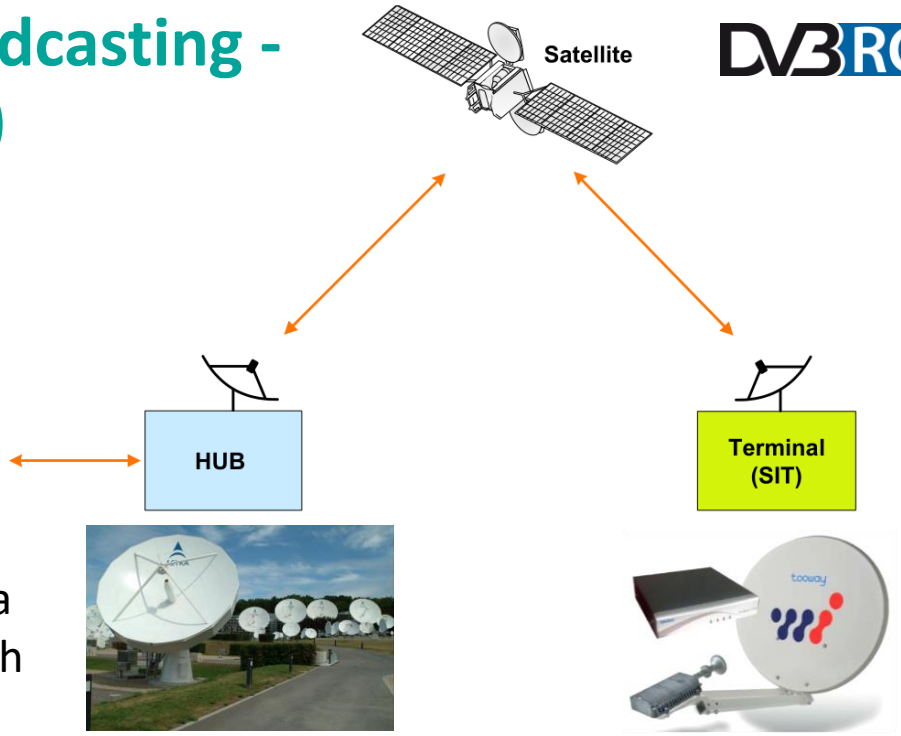


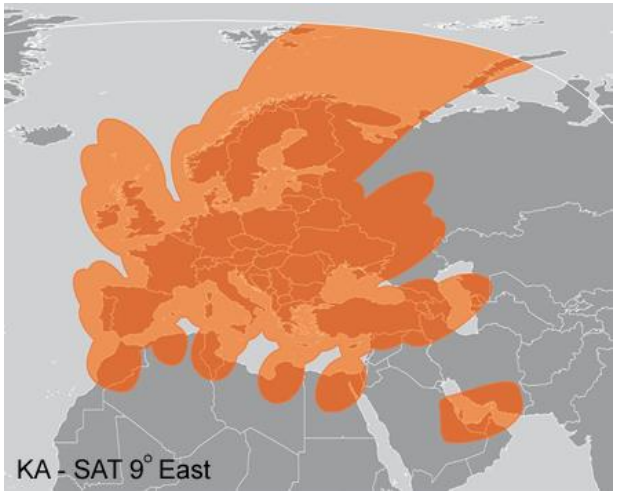
Cluster Tree



DVB-RCS (Digital Video Broadcasting - Return Channel via Satellite)

- ETSI TS 101545, ETSI TS 301545
- defines a complete air interface specification for a two way satellite broadband scheme
- **HUB** - controls the system and acts as a traffic gateway between users and the Internet
- **Terminal (SIT)** - user terminals consist of a small indoor unit and an outdoor unit with an antenna
- **Satellite**
  - high-throughput telecommunications satellite
  - geostationary orbit (altitude approx. 36000 km)
  - *Ku* or *Ka* band
  - EIRP >50dBW, solar array power >10kW
  - total throughput tens of Gbps





source: Eutelsat.com

DVB-RCS Physical Layer

- **Forward Channel (downlink)**
  - QPSK,
  - Ku-band (10,7 GHz - 12,75 GHz)
  - Ka-bank (17,7 – 20,2 GHz)
  - use of TDM
  - up to 80 Mb/s
- **Return Channel (uplink)**
  - QPSK
  - C-band, Ku-band, Ka-band
  - use of MF-TDMA (Multi Frequency - Time Division Multiple Access)
  - up to 8 Mb/s

DVB-RCS2 Physical Layer

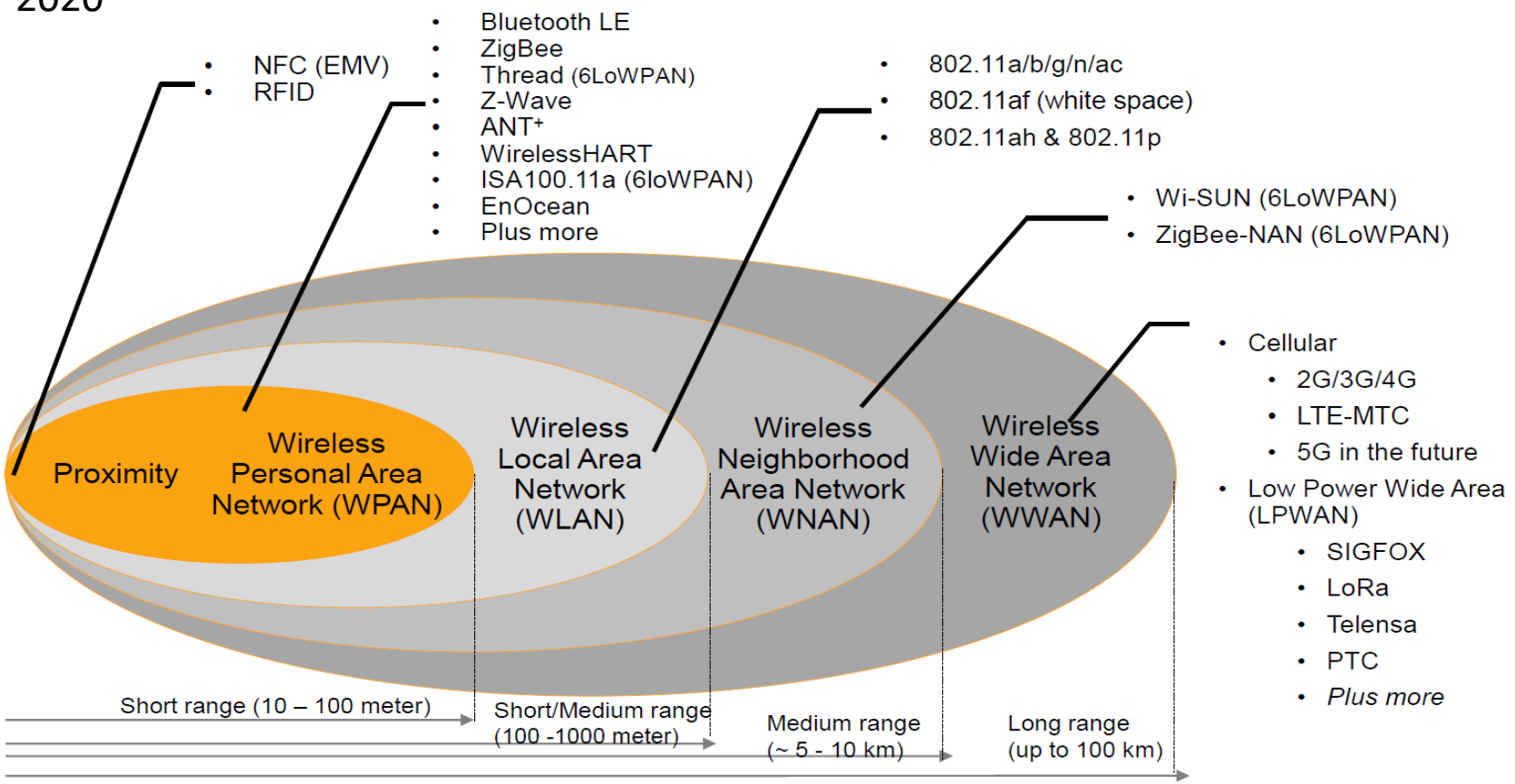
- finished in 2011
- BPSK, QPSK, **8PSK**, **16-QAM**
- **ACM** (Adaptive Coding and Modulation)
- channel coding through highest performance Turbo codes

DVB-RCS Link Layer

- MPEG2 transport stream
- payload may be:
  - IP traffic
  - MPEG2 source coded information, also known as *native MPEG2*

Technology for IoT (Internet of Things)

- A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.
- Cisco estimates the IoT will consist of 50 billion devices connected to the Internet by 2020



Comparison of technologies for IoT

Traditional Cellular

Long Range
Higher data rates
Low battery life
High Cost

LPWAN (3-5B in 2022)

Long Range
Low data rates
Long battery life
Low Cost

Local Area Network

Short Range
High data rates
Low battery life
Medium Cost

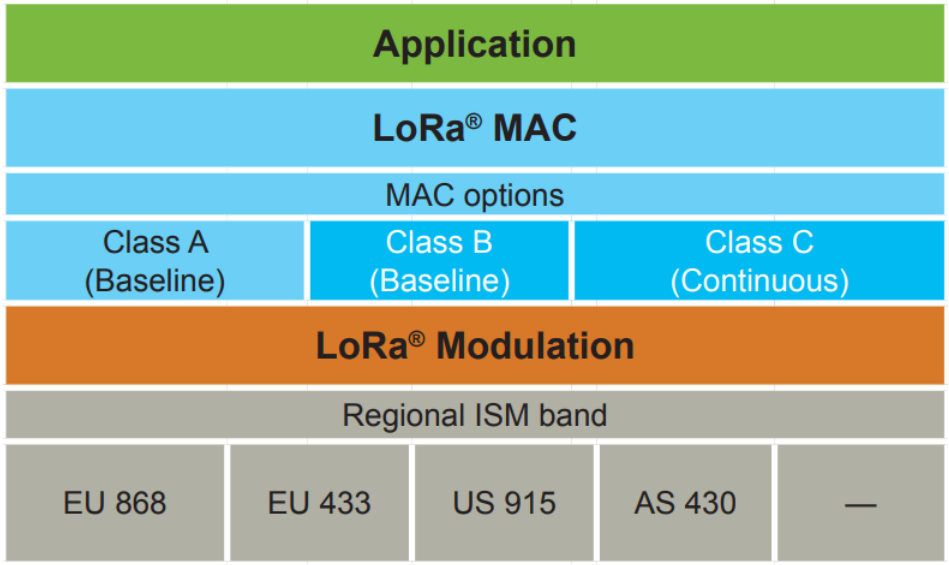
Personal Area Network

Very Short Range
Low data rates
Good battery life
Low Cost

source: semtech.com

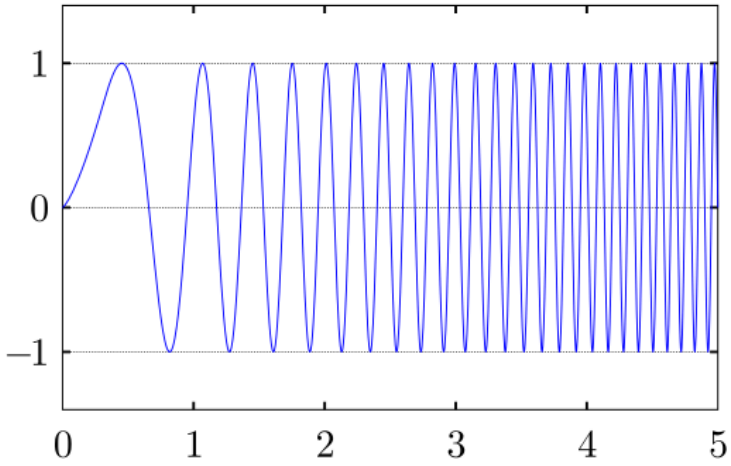
LoRa vs. LoRaWAN

- **LoRa™ -** Physical Layer for LOng RAnge communication, defined by Semtech.
- **LoRaWAN™** - MAC Protocol Layer on top of LoRa™, defined by the LoRa-Alliance, for for Low Power Wide Area Networks (LPWAN).

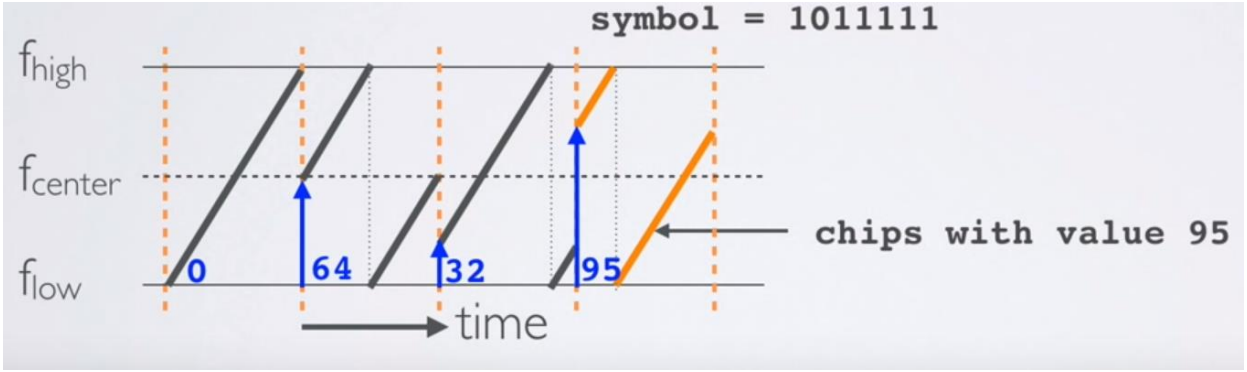


LoRa Physical Layer

- Modulation: FSK + Chirp Spread Spectrum (& FSK)
- Spreading factors: SF7 - SF12
- channel bandwidth 125 kHz
- forward error correction and CRC



example of linear up-chirp



example of sweep signal with SF=7 (128 chips)

$$symbol\ rate = \frac{BW}{2^{SF}}$$

- Higher the Spreading Factor → Higher the over-the-air time
- Lower the Spreading Factor → Higher the Data Rate.

LoRa Duty Cycle

In Czech Republic, **operation in 868 MHz band must fulfil General License requirements** released by ČTÚ, **„Všeobecné oprávnění č. VO-R/10/01.2019-1“**
https://www.ctu.cz/vseobecne-opravneni-c-vo-r10012019-1

Duty cycle is defined

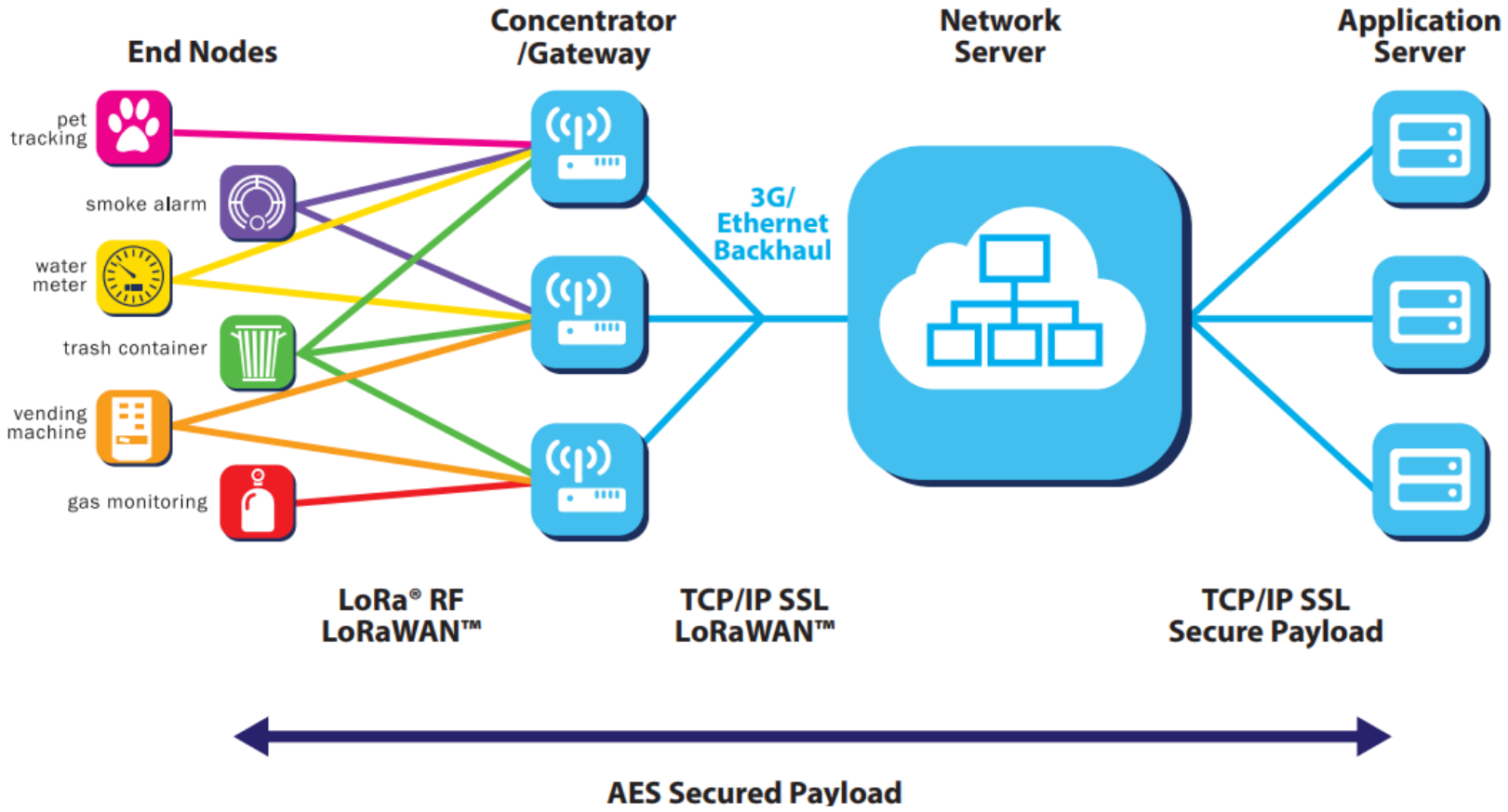
„Klíčovací poměr (duty cycle) je podíl času, kdy zařízení aktivně vysílá, v rámci jakékoliv jedné hodiny, není-li v příslušném článku určeno jinak. Podrobná definice klíčovacího poměru je uvedena v ERC-REC 70-034) a v harmonizovaných normách.“

g	863,0–870,0 MHz	25 mW e.r.p.	viz odst. 4	odst. 4, 7 nebo ≤ 0,1 %[9]),	3, 4, 7, 8 (FHSS[10]))

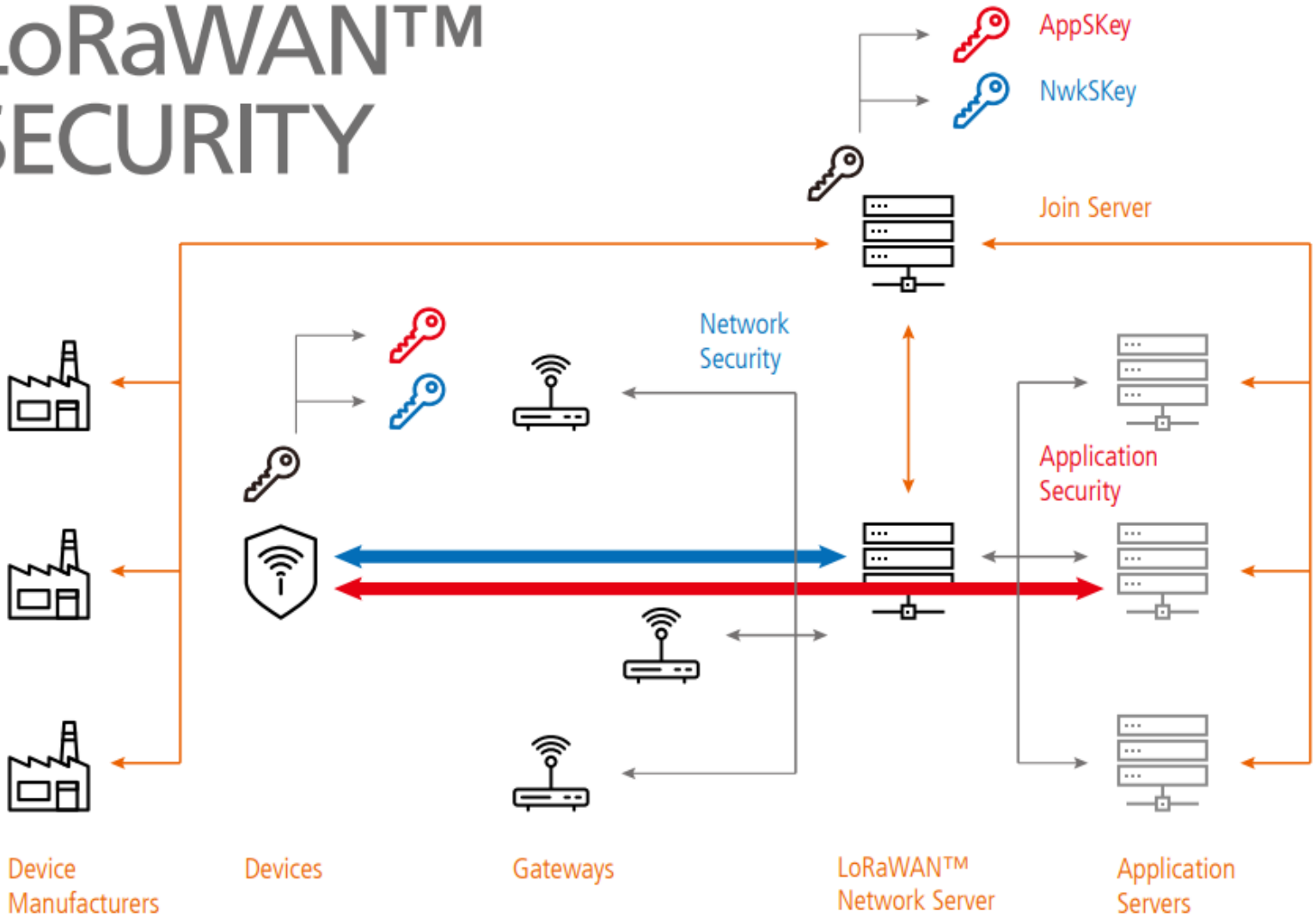
Frequency plan (EU863-870)

1. 868.1 MHz (SF7@BW125 - SF12@BW125)
2. 868.3 MHz (SF7@BW125 - SF12@BW125 and SF7@BW250)
3. 868.5 MHz (SF7@BW125 - SF12@BW125)
4. 867.1 MHz (SF7@BW125 - SF12@BW125)
5. 867.3 MHz (SF7@BW125 - SF12@BW125)
6. 867.5 MHz (SF7@BW125 - SF12@BW125)
7. 867.7 MHz (SF7@BW125 - SF12@BW125)
8. 867.9 MHz (SF7@BW125 - SF12@BW125)
9. 868.8 MHz (only FSK)

LoRaWAN Network Architecture



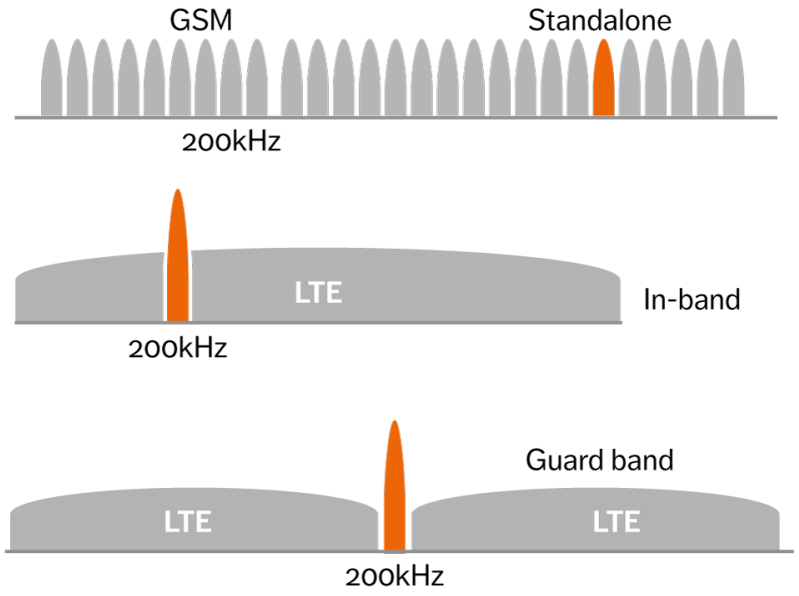
LoRaWAN™ SECURITY



source: LoRa-Alliance, LoRaWAN security whitepaper

NB-IoT (Narrow Band IoT)

- Narrowband LPWAN under 3GPP
- Closed technology in licensed bands
- As a part of GSM or LTE in 200 kHz bandwidth
- In Czech Republic – Vodafone and T-Mobile



LPWAN Technologies Overview

	Sigfox	LoRa	NB-IoT
Standardization	Private	Open	3GPP
Frequency	868 MHz (Unlicensed)	868 MHz (Unlicensed)	3GPP Band 20 (Licensed)
Modulation	DBPSK	FSK (Chirp Spectrum)	QPSK
Channel Bandwidth	100 Hz	8 x 125 kHz	180 KHz
Peak Data Rate	UL: 100bps DL: 600bps	250 bps – 5470 bps (SF0-SF7)	DL: 234.7kbps UL: 204.8kbps
Max. number of messages per day	140 (Device)	unlimited	unlimited
Message Size	0-12 Bytes	59 - 250 Bytes	1600 Bytes
Device Peak Tx Power	14dBm	14dBm	23dBm

- the goal of the project is to build an academic experimental network of the Internet of Things using open gateway platforms and network terminal equipment,
- custom gateway development,
- we use **LoRaWAN** ™ standard in **868 MHz** license-free band,
- extremely low power consumption (LPWAN technology),
- compared to the available competitive networks, **our service is open**, anyone can connect and operate their sensors for free,
- all gateways connected to The Things Network (TTN)
- own web portal https://lora.vsb.cz/ (sensor registration, instructions, procedures, experiences, ...)

References

- Gast, M.. 802.11 Wireless Networks: The Definitive Guide. Definitive Guide Series.O'Reilly Media, 2005. ISBN 9780596100520.
- Perahia, E.. and Stacey, R.. Next Generation Wireless LANs: 802.11n and 802.11ac. Next Generation Wireless LANs: 802.11n and 802.11ac. Cambridge University Press, 2013. ISBN 9781107016767.
- Chaouchi, H.. and Laurent-Maknavicius, M.. Wireless and Mobile Networks Security. ISTE. Wiley, 2013. ISBN 9781118619544.
- Morrow, R.. Bluetooth: Operation and Use: Operation and Use. McGraw-Hill telecom professional. McGraw-Hill Education, 2002. ISBN 9780071409636.
- Bluetooth Specifications. https://www.bluetooth.com/specifications/bluetooth-core-specification
- ZIGBEE SPECIFICATION, Zigbee Alliance, http://www.zigbee.org
- Gislason, D.. Zigbee Wireless Networking. Elsevier Science, 2008. ISBN 9780080558622.
- IEEE Standard for Air Interface for Broadband Wireless Access Systems. IEEE Std 802.16-2012. IEEE, 2012.
- ETSI EN 301 790 V1.5.1 (2009-05): Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems. ETSI, 2009.
- ETSI TS 101 545-1 V1.2.1 (2014-04): Digital Video Broadcasting (DVB); Second Generation DVB, Interactive Satellite System (DVB-RCS2); Part 1: Overview and System Level Specification. ETSI, 2014.
- ETSI TS 101 545-2 V1.2.1 (2014-04): Digital Video Broadcasting (DVB); Second Generation DVB, Interactive Satellite System (DVB-RCS2); Part 2: Lower Layers for Satellite Standard. ETSI, 2014.
- ETSI TS 101 545-3 V1.2.1 (2014-04): Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 3: Higher Layers Satellite Specification. ETSI, 2014.
- LoRaWAN™ Specification v1.1. https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf