Wireless Access Networks

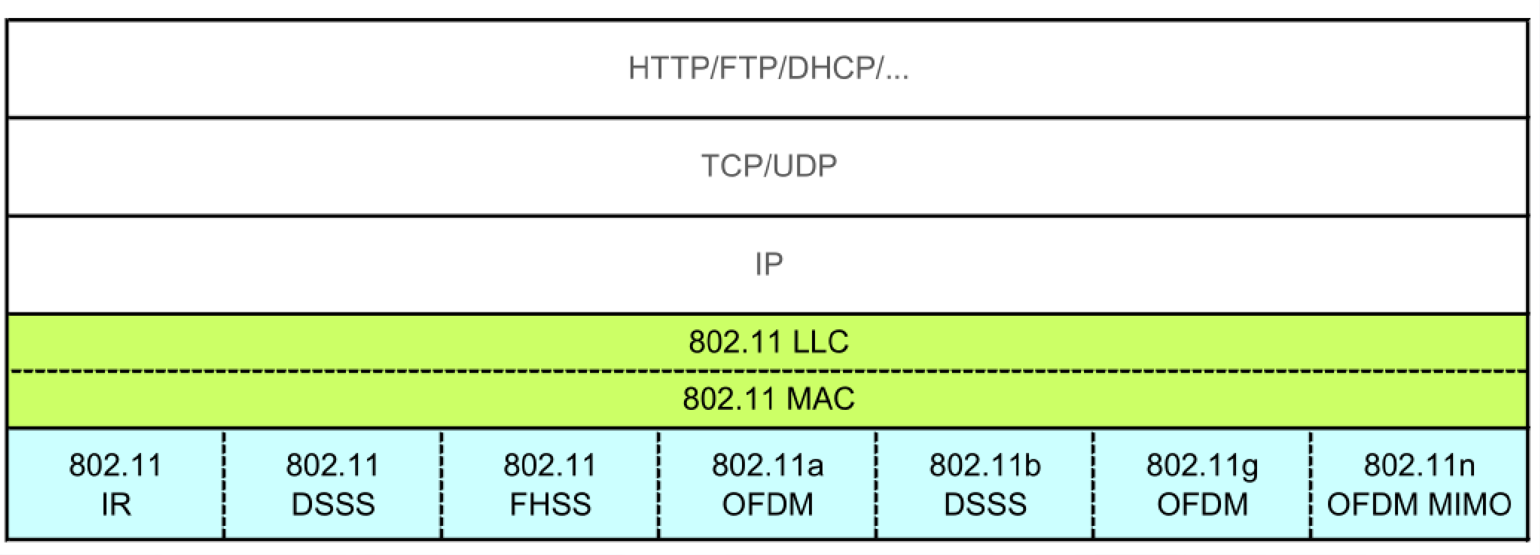
Libor Michalek

2017

Department
of Telecommunications

WLAN Technology

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



HTTP/FTP/DHCP/...

TCP/UDP

IP

802.11 LLC

802.11 MAC

802.11 IR	802.11 DSSS	802.11 FHSS	802.11a OFDM	802.11b DSSS	802.11g OFDM	802.11n OFDM MIMO

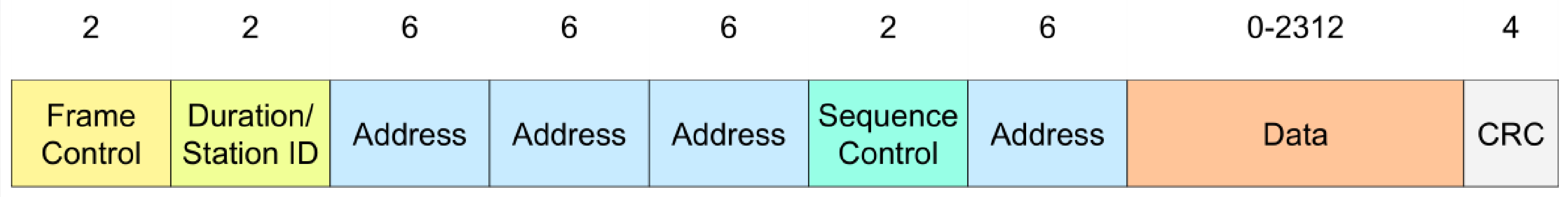
Physical Layer

- the physical layer defines the spectrum technique and modulation
- ISM band 2400-2483,5 MHz
  - **FHSS** (Frequency Hopping Spread Spectrum)
    - 79 channels, each 1MHz
    - 400 ms is time fo transmitting
    - lower bitrates than DSSS
  - **DSSS** (Direct Sequence Spread Spectrum)
    - 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

Link Layer

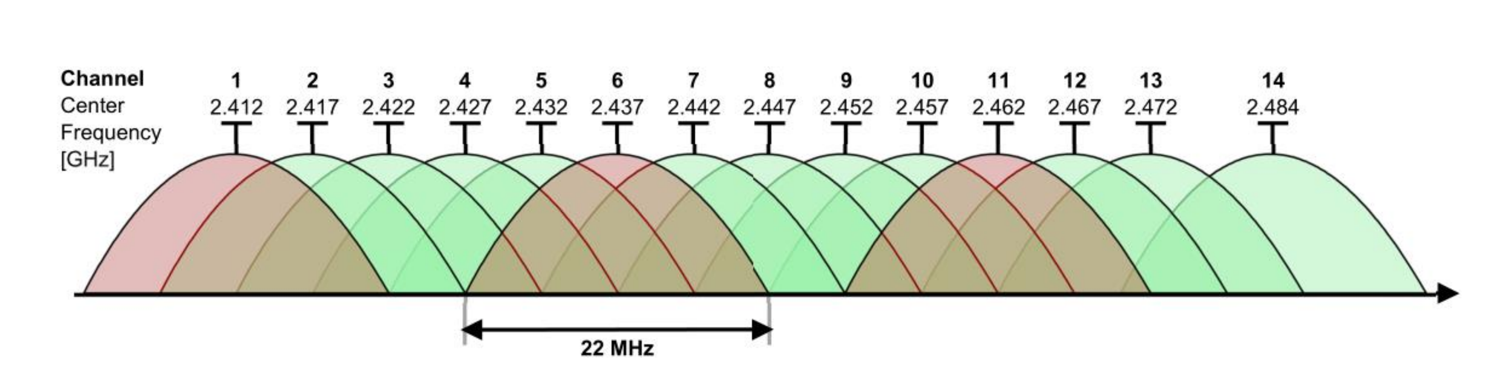
- defines structure of frame, access method, multiplexing technique, error protection and ciphering
- two sublayers are defined:
  - **LLC** (Logical Link Control)
  - **MAC** (Media Access Control)
- **MAC layer**
  - defines access method, frame structure and protection
  - Access Methods
    - **DCF** (Distributed Coordination Function), based on CSMA/CA
    - **RTS/CTS** (Request To Send / Clear To Send)
    - **PCF** (Port Coordination Function)

- 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



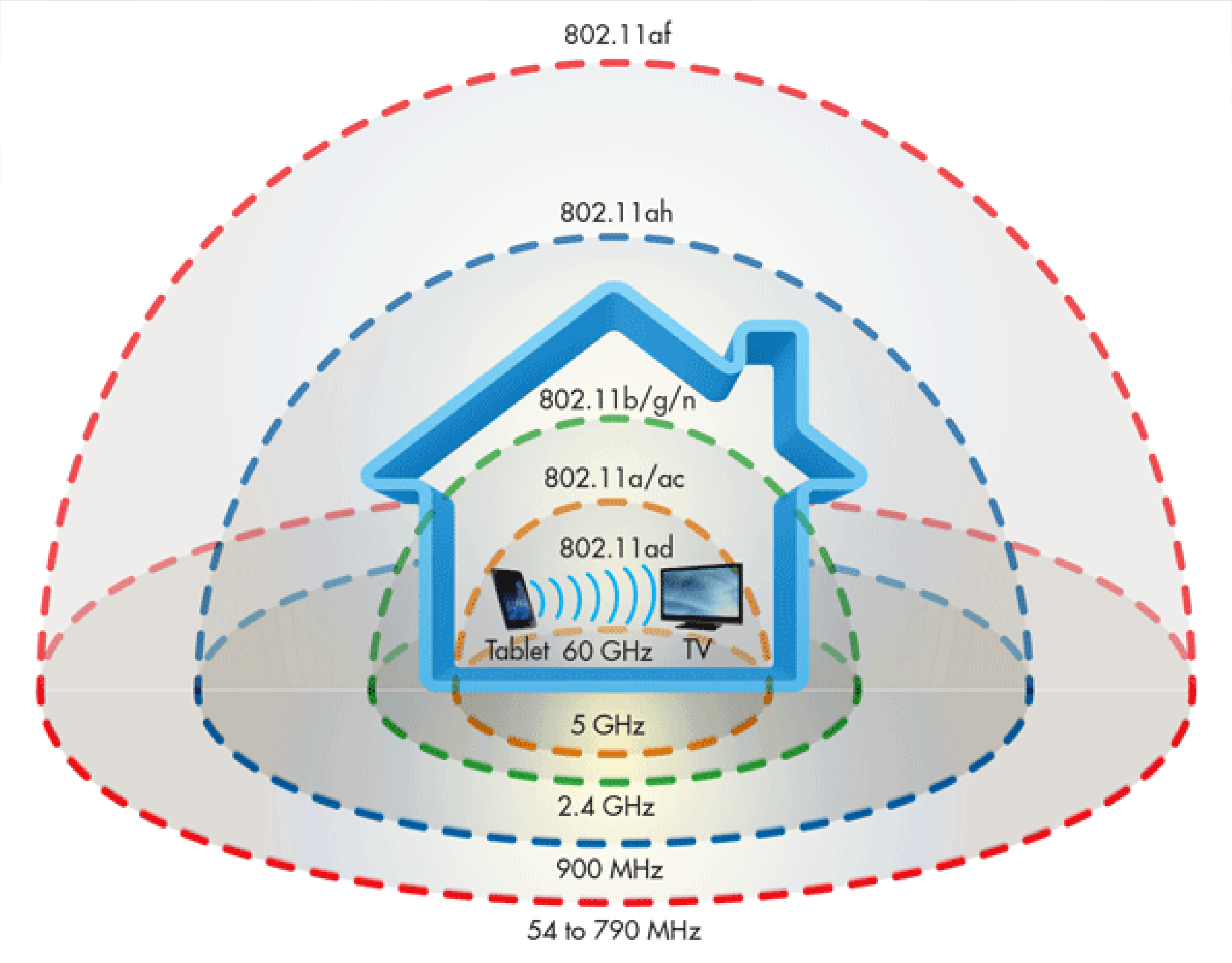
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ Station ID	Address	Address	Address	Sequence Control	Address	Data	CRC

- IEEE 802.11 defines the family of specifications:
  - **802.11**
    - applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS)
  - **802.11a**
    - an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band
  - **802.11b**
    - 1999, 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



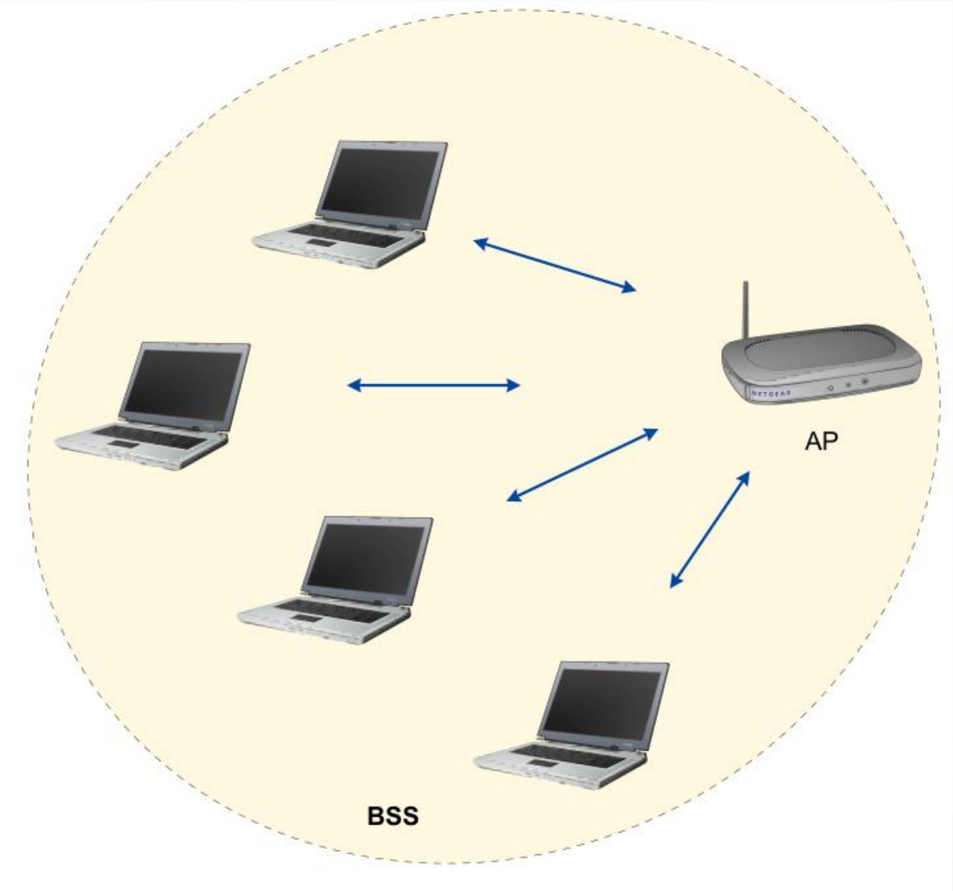
- **802.11g**
  - uses the OFDM, back compatibility to 802.11b
  - up to 54 Mb/s
- **802.11n**
  - builds upon previous 802.11 standards by adding *MIMO (multiple-input multiple-output)*
  - MIMO is a method for multiplying the capacity of a radio link using multiple transmit and receive antennas to exploit multipath propagation
  - offers high throughput wireless transmission at 100Mbps – 200Mbps.
- **802.11ac**
  - reservation of mulitple 20 MHz channels
  - primary 20 MHz channel is always choosen (transmitting of **Beacon**)
  - total bandwidth is adaptivelly changes based on actual level in interference
  - up to 160 MHz
  - up to 256-QAM

- **802.11ad**
  - in2008 **TGad** workgroup under IEEE established
  - addon to 802.11 with the aim of working in 60 GHz band
  - also as **WiGig**
  - up to 7 Gb/s.
- **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 requency band and range for 802.11 family standards

- 802.11 standard defines two operating modes:
  - **Infrastructure mode** - in which 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

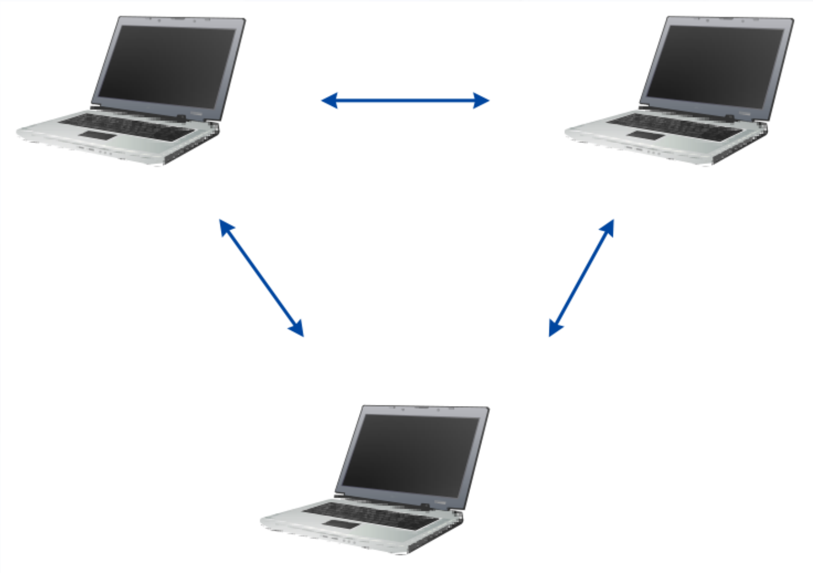


Fig. IEEE 802.11 Ad Hoc mode

WLAN Network Security

- **SSID blocking**
- **Filtering MAC addresses**
  - 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**
  - data frame encryption protocol that uses the symmetrical algorithm RC4 with 64-bit or 128-bit keys
  - cracked!

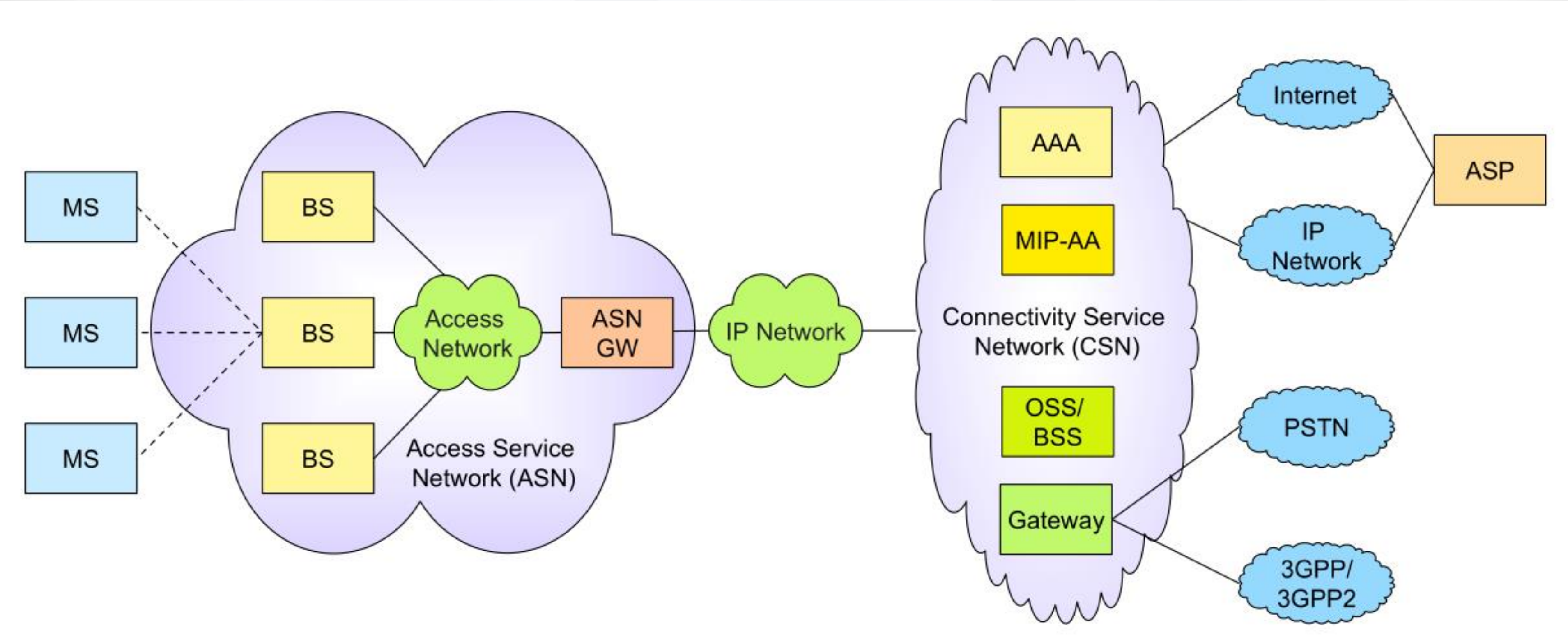
- **WPA - WPA - WiFi Protected Access**
  - relies on a strong encryption algorithm TKIP (Temporary Key Integrity Protocol)
  - TKIP generates keys randomly and can alter an encryption key several times a second, for greater security

- **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)
- **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 is 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

- system architecture



- Three main parts in architecture:
  - **MS** (Mobile Station)
  - **ASN** (Access Service Network)
  - **CSN** (Connectivity Service Network)

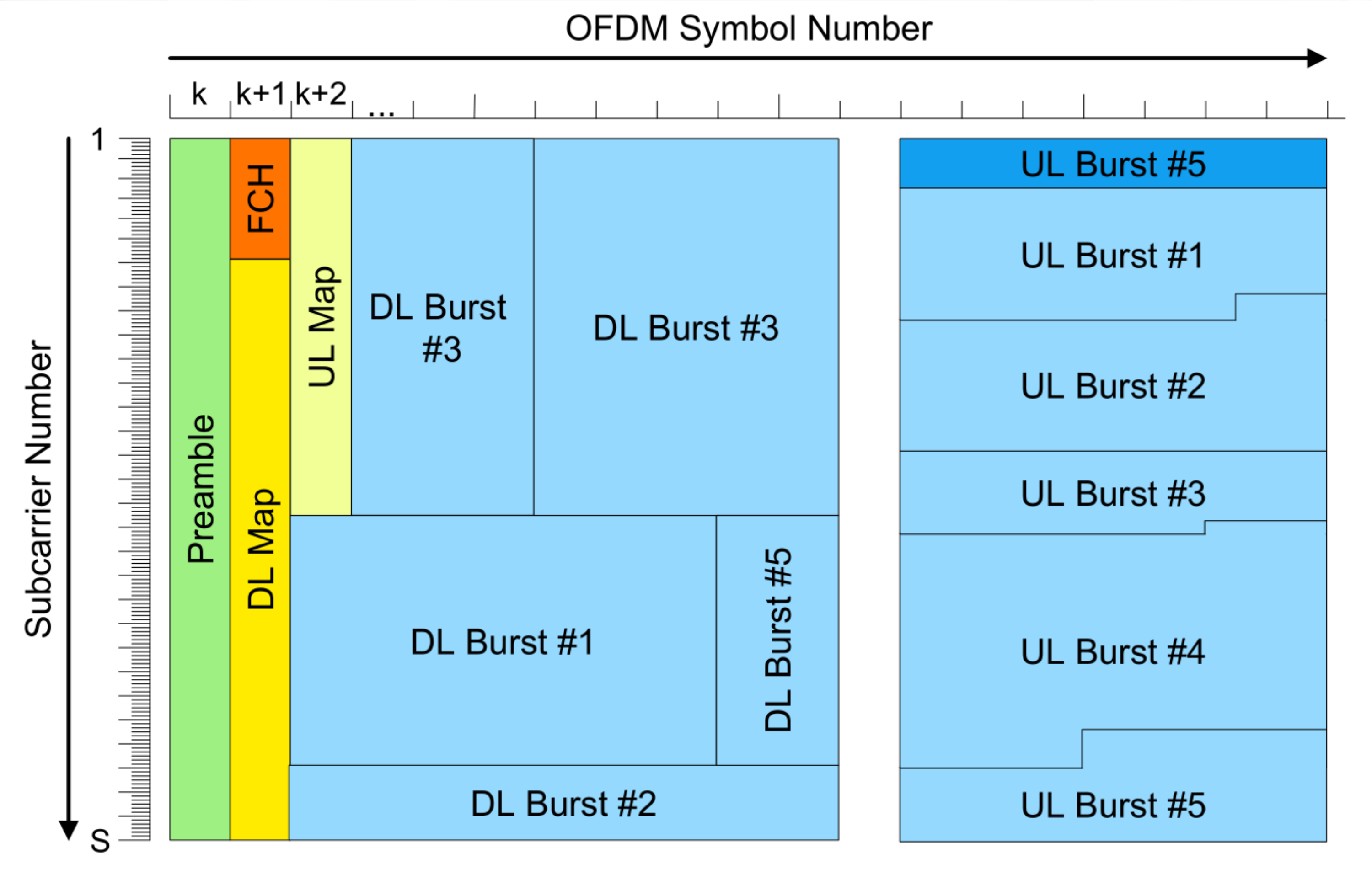
- BS (Base Station)
- ASN-GW (Access Service Network Gateway)
- CSN (Connectivity Service Network)

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

MAC Layer

- time-frequency map is defined, in which the **frames** are transmitted

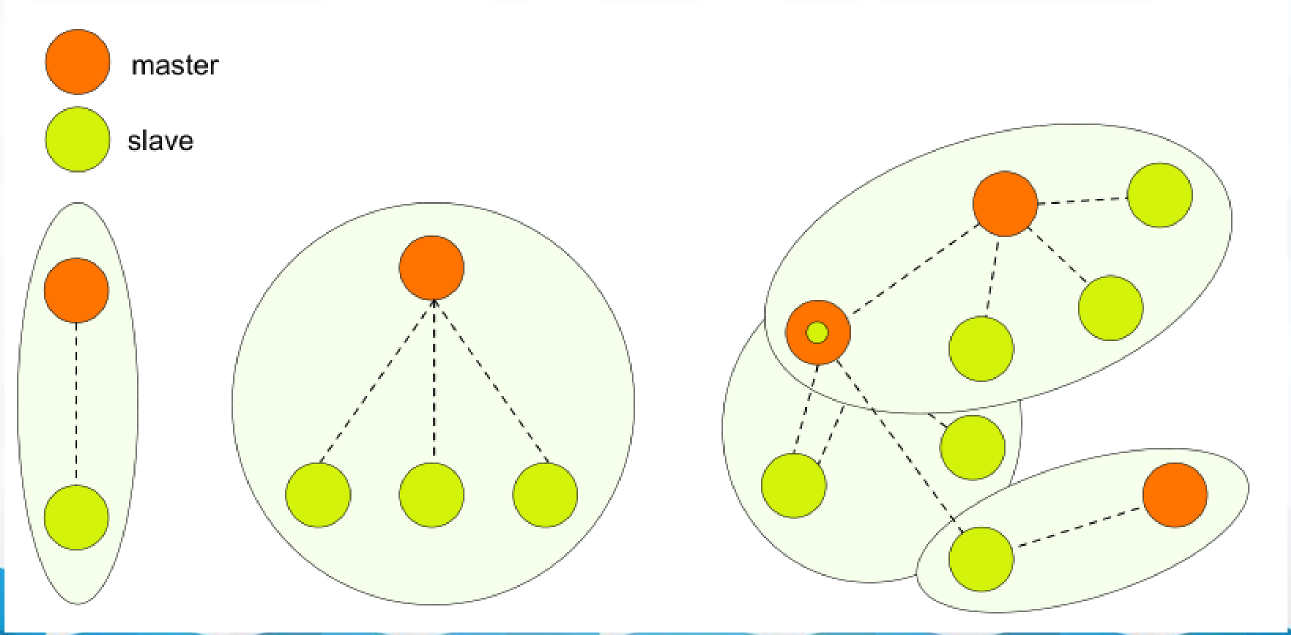


Bluetooth

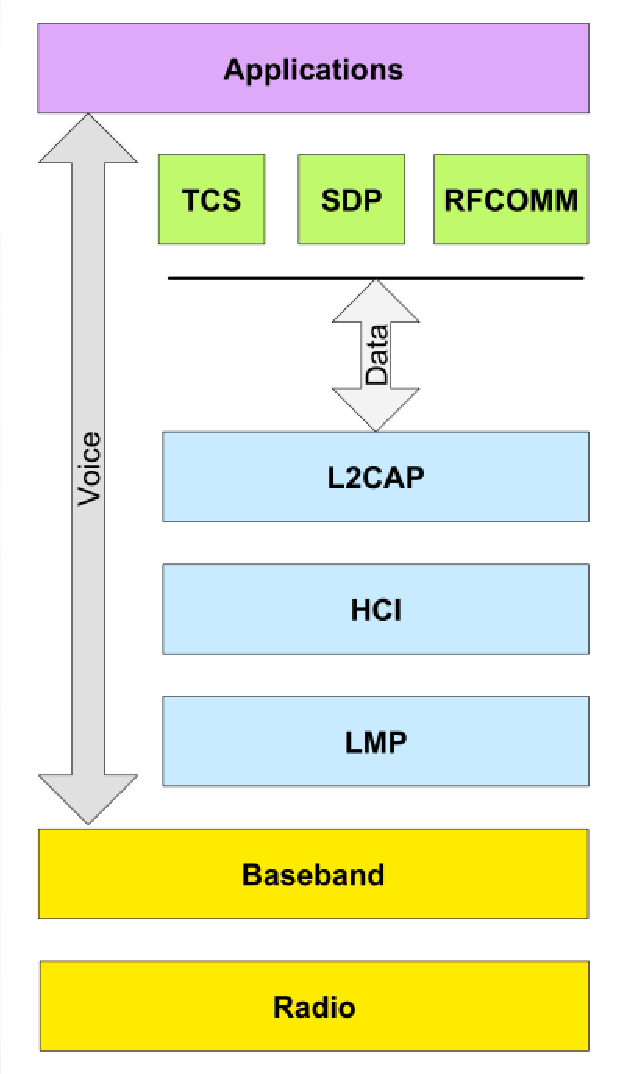
- Wireless Personal Area Network Technology (WPAN)
- low-range wireless network technology used for linking devices to one another without a hard-wired connection
- do not need a direct line of sight to communicate
- he aim is to transmit voice or data between devices with low-cost radio circuits, over 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

Operational modes

- **master - slave**
- **piconet**
  - a master can be simultaneously connected to as many as 7 active slave devices
- **scatternet**
  - scatternets can be formed when a member of one piconet (either the master or one of the slaves) elects to participate as a slave in a second, separate piconet

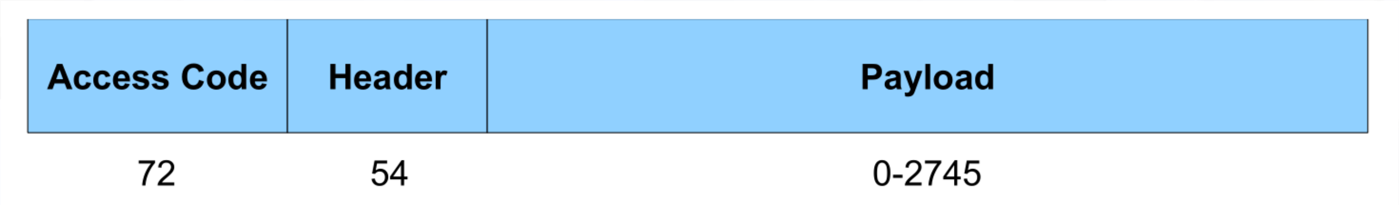


Protocol stack



- **Bluetooth radio**
  - 2,4 GHz frequency band
  - GFSK (Gaussian Frequency Shift Keying) modulations with 1000 kBd,
  - the 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 *(FHSS)* 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
- **LMP (Link Manager Protocol)**
  - for procedures such as Inquiry, Paging and Pairing

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



Access Code	Header	Payload
72	54	0-2745

  - 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

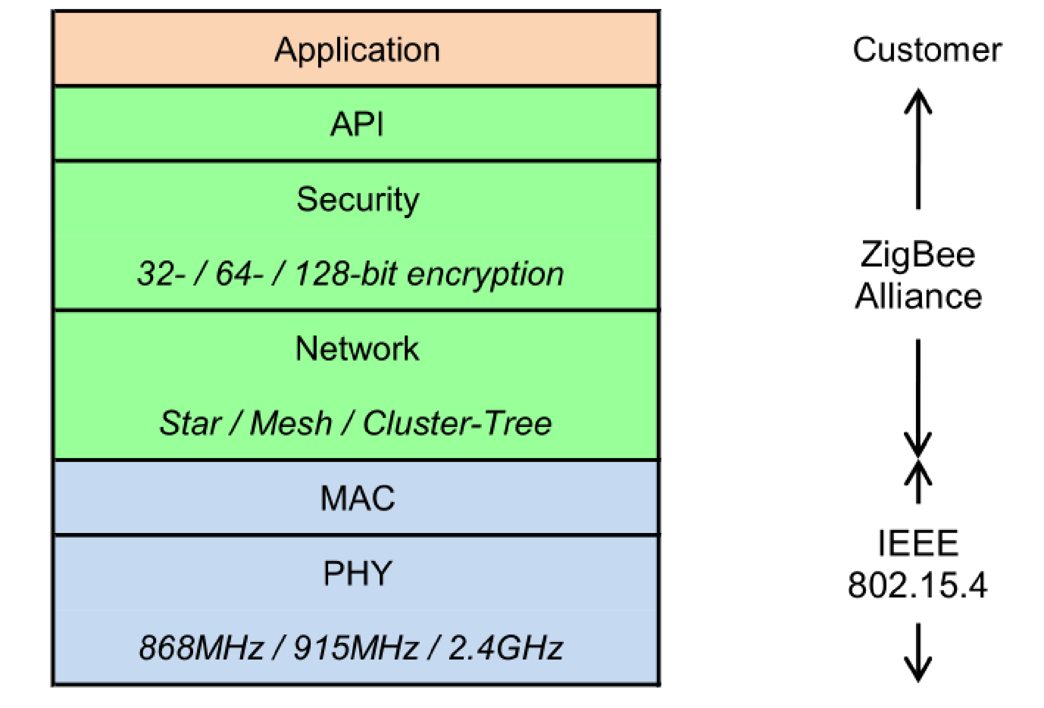
- Bluetooth 1.0 and 1.0B
- Bluetooth 1.1
- Bluetooth 1.2
- Bluetooth 2.0
- Bluetooth 2.1
- Bluetooth 3.0
- Bluetooth 4.0 (as BLE)
- Bluetooth 4.1
- Bluetooth 4.2
- Bluetooth 5 (2017)

Zigbee

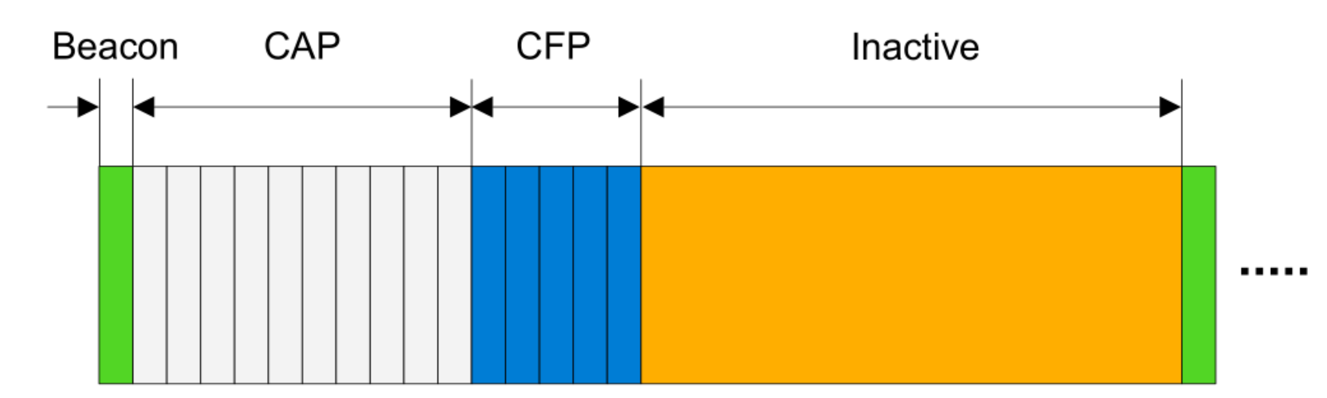
- specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard
- wireless personal area network (WPAN), such as wireless headphones connecting with cell phones via short-range radio
- simpler and less expensive than other WPANs, such as Bluetooth
- low-cost, low-power, wireless mesh networking standard
- operates in the industrial, scientific and medical (ISM) radio bands

Protocol Stack

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

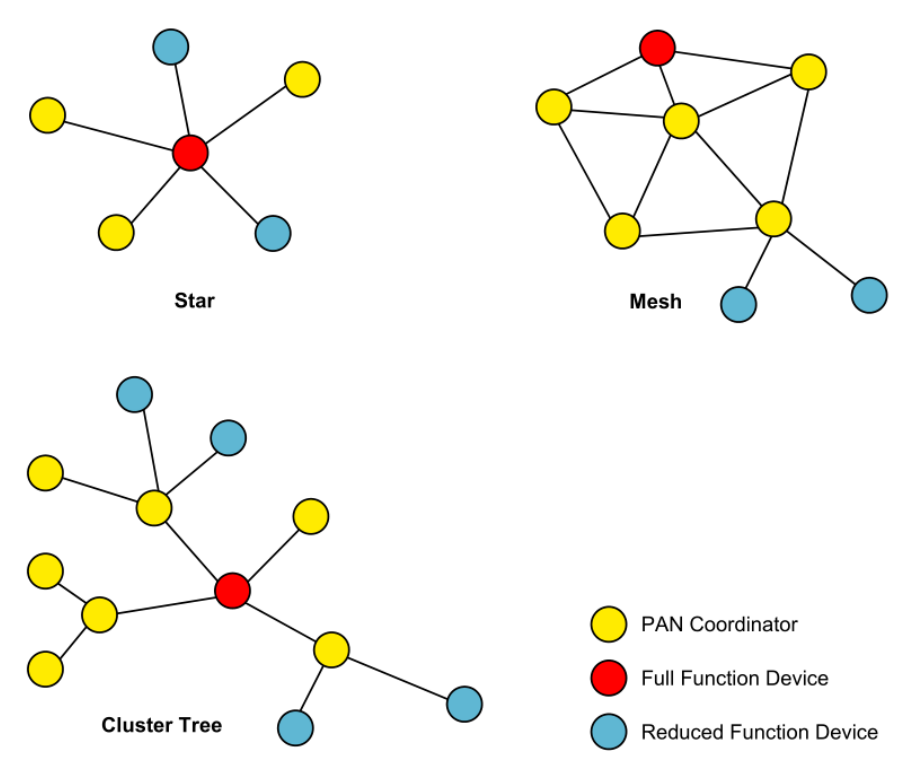


- **Physical Layer**
  - use of BPSK or QPSK
  - working band: 868 MHz, 902-928 MHz, 2400 MHz
- **MAC layer**
  - synchronization, error protection, ciphering, management of frames
  - frames divides into
    - Beacon
    - CAP (Contention Access Period) and CFP (Contention Free Period)
    - Inactive – low power mode



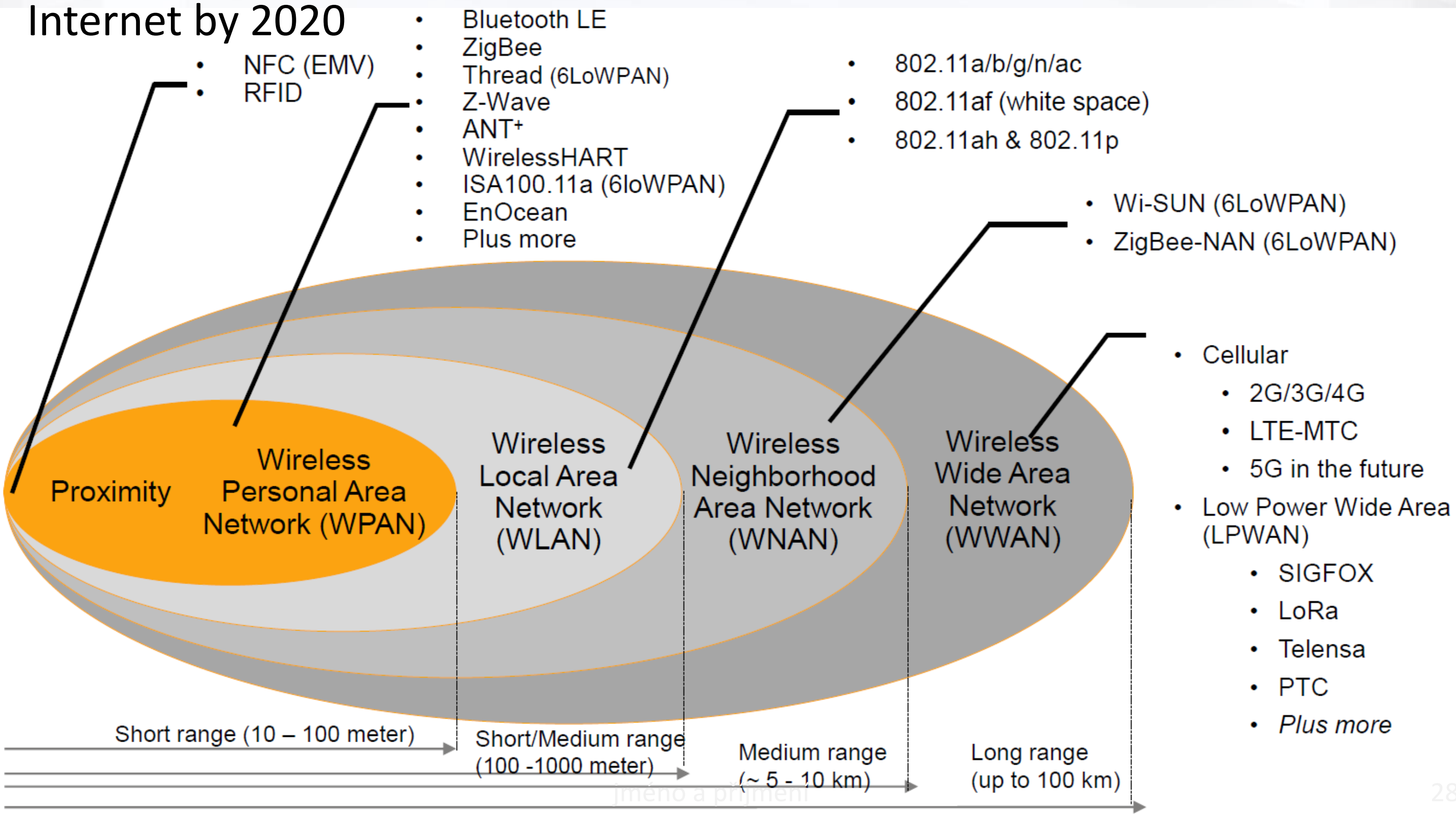
Topology

- support of star, tree and mesh topology
- node can operate as either a full-function device (FFD) or reduced-function device (RFD).
- coordinator is an FFD and responsible for overall network management
- end device can be an RFD



Technology for IoT

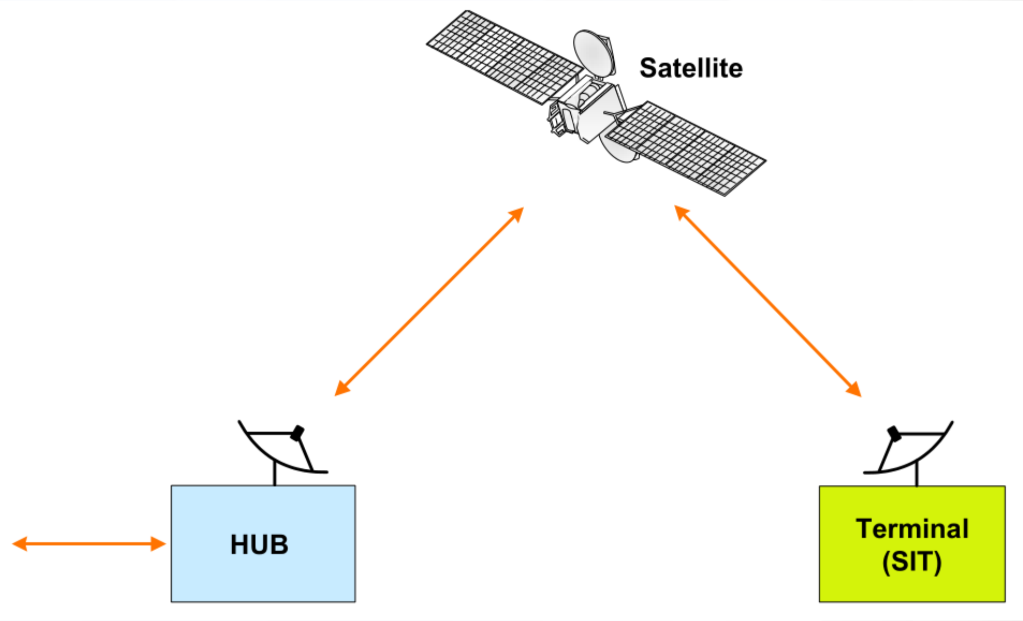
- A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.
- Cisco estimates the IoT will consist of 50 billion devices connected to the Internet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



NFC (EMV)
RFID
Bluetooth LE
ZigBee
Thread (6LoWPAN)
Z-Wave
ANT+
WirelessHART
ISA100.11a (6loWPAN)
EnOcean
Plus more
802.11a/b/g/n/ac
802.11af (white space)
802.11ah & 802.11p
Wi-SUN (6LoWPAN)
ZigBee-NAN (6LoWPAN)
Cellular
2G/3G/4G
LTE-MTC
5G in the future
Low Power Wide Area (LPWAN)
SIGFOX
LoRa
Telensa
PTC
Plus more
Proximity
Wireless Personal Area Network (WPAN)
Wireless Local Area Network (WLAN)
Wireless Neighborhood Area Network (WNAN)
Wireless Wide Area Network (WWAN)
Short range (10 – 100 meter)
Short/Medium range (100 -1000 meter)
Medium range (~ 5 - 10 km)
Long range (up to 100 km)

DVB-RCS

- Digital Video Broadcasting - Return Channel via Satellite
- it defines a complete air interface specification for a two way satellite broadband scheme
- **DVB-RCS HUB**
  - controls the system and acts as a traffic gateway between users and the Internet
- **DVB-RCS terminal**
  - User terminals consist of a small indoor unit, and an outdoor unit with an antenna

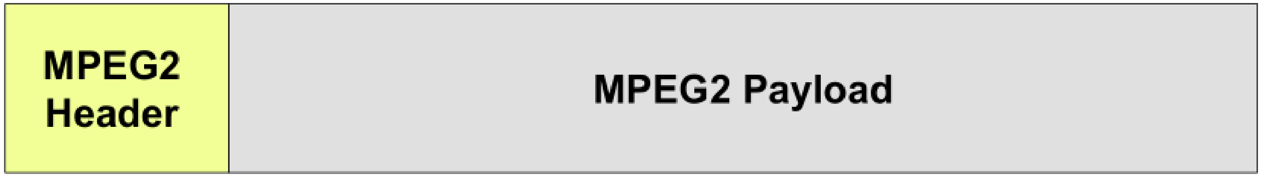


Physical Layer

- **Forward Channel**
  - direction HUB → Transponder → Terminal
  - QPSK
  - C-band, Ku-band, Ka-band
  - Ku-band most used (10,7 GHz - 12,75 GHz)
  - use of TDM
  - use of conventional DVB/MPEG2 frame
  - up to 80 Mb/s
- **Return Channel**
  - Terminal → Transponder → HUB
  - QPSK
  - C-band, Ku-band, Ka-band
  - Ku-band most used (10,7 GHz - 12,75 GHz)
  - use of MF-TDMA (Multi Frequency - Time Division Multiple Access
  - up to 8 Mb/s

Transport stream

- MPEG2 has been universally adopted by DVB in all its varieties for source coding of video, audio and associated data information and for transmitting various source data streams in digital wrappers, also called digital containers
- the **payload** may be:
  - IP traffic
  - MPEG2 source coded information, also known as “native MPEG2”
  - other bitstreams that comply with TCP/UDP



DVB-RCS2

- finished in 2011
- main improvements:
  - BPSK, QPSK, **8PSK, 16-QAM**
  - **ACM** (Adaptive Coding and Modulation)
  - use of **Turbo-code**

DECT

- Digital Enhanced Cordless Telecommunications
- ETSI standard for digital portable phones (cordless home telephones)
- band 1880 MHz–1900 MHz is used
- 10 carriers with span of 1728 kHz
- FDMA/TDMA frame, where ona frame is divided into 24 timeslots (2 x 12 up and down stream)
- audio codec G.726
- average transmission power 10 mW (250 mW peak) in Europe
- DECT Standard Cipher (DSC) used, the encryption is fairly weak, security algorithm has been broken

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.
- IEEE Standard for Air Interface for Broadband Wireless Access Systems. IEEE Std 802.16-2012. IEEE, 2012. https://standards.ieee.org/about/get/802/802.16.html
- 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.
- ETSI EN 300 444 V2.4.1 (2013-07) Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP). ETSI, 20013.