IoT

Fundamentals, architecture and protocols

Course id: IOTG

2021

∴

Eric Gaillard

Teaching carried out in GISTRE under the responsibility of Pierre Ficheux

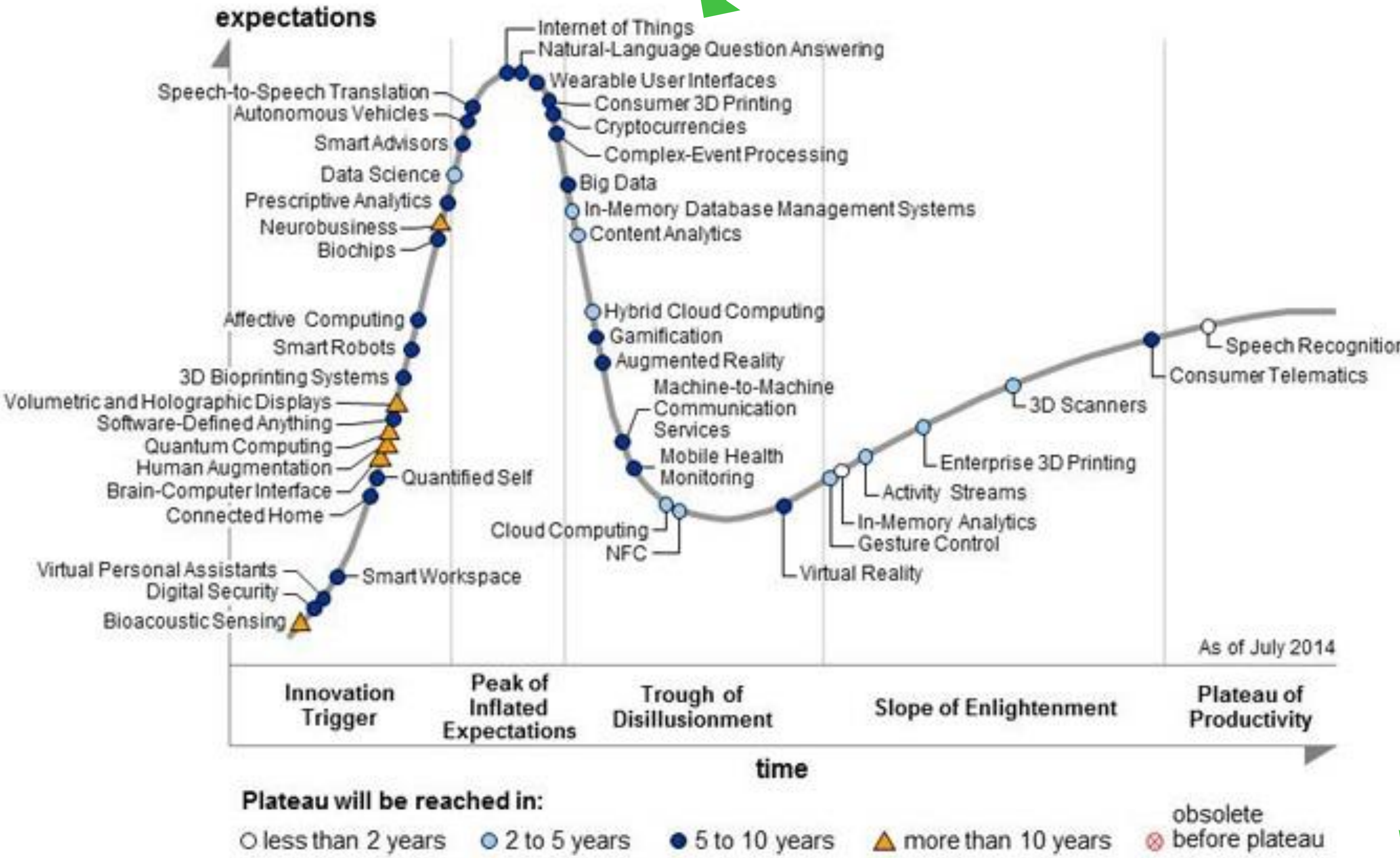
This course material usually comes along with oral explanations
This course is not intended to replace the reference documents, whose reading is highly recommended.
Neither it is to be a substitute of an operational practice

Content

- Internet of Things
- IoT Architecture / Cloud, Edge, Fog Computing
- Connectivity & protocols
- IoT Market
- IoT Security
- Case study
- Exercises
- References

Internet of Things: definitions

- A single concept, various names and definitions
  - “Internet of Everything”
  - “World Size Web”
  - “Skynet”
  - …
- IEEE
  - “An IoT system is a network of networks where, typically, a massive number of objects, things, sensors or devices are connected through communications and information infrastructure to provide value-added services via intelligent data processing and management for different applications (e.g. smart cities, smart health, smart grid, smart home, smart transportation, and smart shopping).”
- McKinsey
  - “The physical world itself is becoming a type of information system. In what’s called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What’s revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention.”
- ITU
  - “IoT is a concept encompassing various platforms, applications, and technologies implemented under a number of radio communication services”
- A famous acronym … IoT



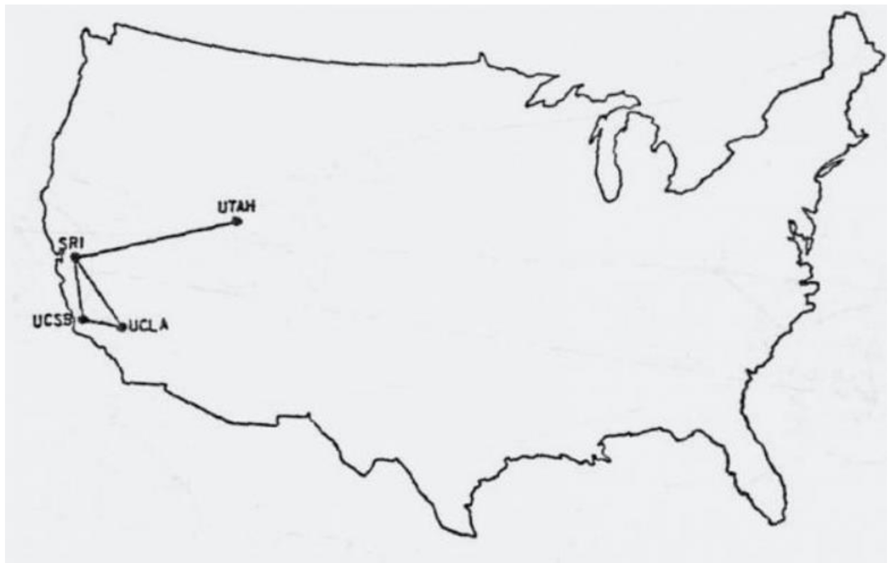
Source: Gartner, Aug 2014

- “The original ‘Internet’ is based on the TCP/IP protocol suite, but any network based on the TCP/IP protocol suite cannot belong to the Internet because private networks and telecommunication networks are not part of the Internet even though they are based on the TCP/IP Protocol suite. In the viewpoint of IoT, the ‘Internet’ considers the TCP/IP suite and non-TCP/IP suite at the same time.”
- 1969


Leonard Kleinrock

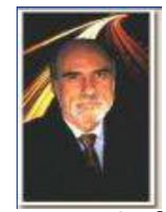

Lawrence Roberts


Steve Crocker



The ARPANET in December 1969


Robert Kahn


Vinton Cerf


Jon Postel

- And today …

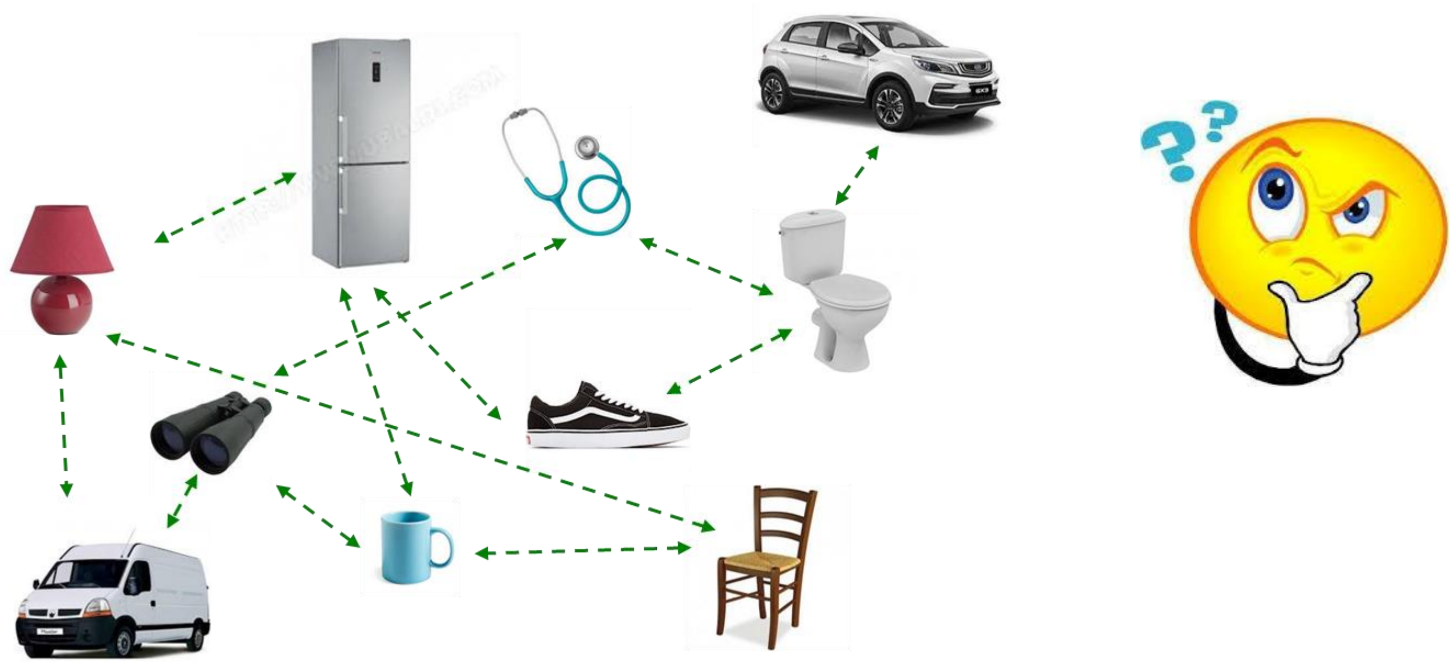
- ...

Tim-Berners Lee

Ted Nelson

Mark Andreesen

- Things Definition (Source Larousse)
  - *Chose solide considérée comme un tout, fabriquée par l'homme et destinée à un certain usage*
  - *Chose inerte, sans pensée, sans volonté et sans droits, par opposition à l'être humain*
- …
- Every connected object



- IETF
  - “In the vision of IoT, ‘things’ are very various such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc. These things are classified as three scopes: people, machine (for example, sensor, actuator, etc.) and information (for example, clothes, food, medicine, books, etc.). These ‘things’ should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. In here, if the ‘thing’ is identified, we call it the ‘object.

- ITU-T definition
  - Physical things

    Exist in the physical world and are capable of being sensed, actuated and connected.

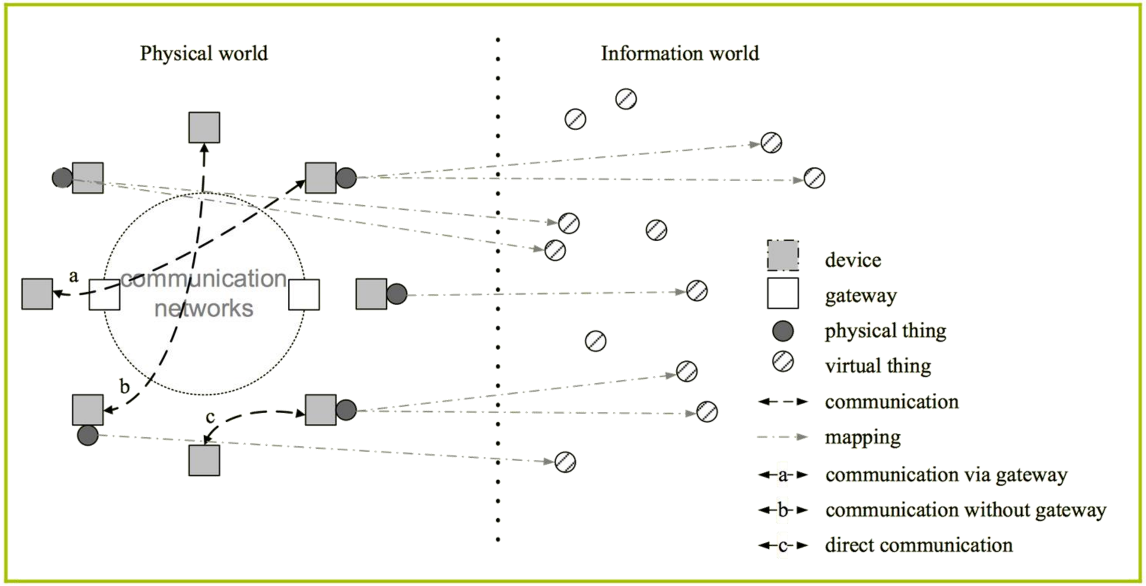
    Examples: industrial robots, goods and electrical equipment.

  - Virtual things

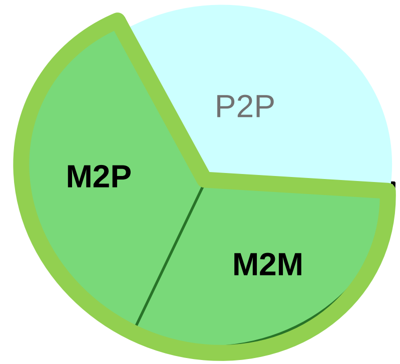
    Exist in the information world and are capable of being stored, processed and accessed.

    Examples: Multimedia content, application software.

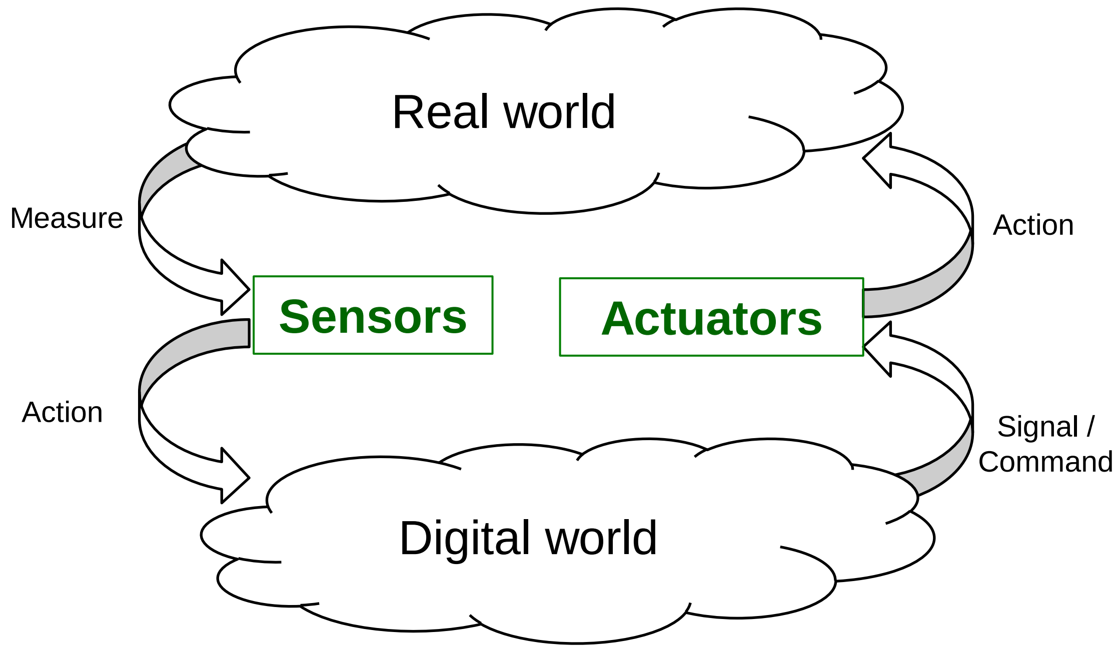
- Anywhere, anytime, any business, Any usage, anyone, any things



Source: Recommendation ITU-T Y.2060



- Interface
  - Real world
  - Digital world
- Sensors / Actuators



- Any Size, any shape, embedded or not
- Sensor type
  - Accelerometer sensors
  - Acoustic
  - Altitude
  - Biosensor
  - Chemical
  - Color
  - Flow
  - Force
  - Gas sensors
  - Gyroscope sensors
  - Humidity
  - Infrared sensors
  - Level sensors
  - Light
  - Magnetic field
  - Motion
  - Occupancy
  - Optical sensors
  - pH
  - Position
  - Pressure
  - Proximity
  - Radiation
  - Temperature
  - Velocity
  - Viscosity
  - …

IoT: OS for things

Nom de l'OS	Date de creation	Version à date	Langage de program-mation	Licence	Sources
Amazon FreeRTOS	2017	10.3.x	C	MIT	https://www.freertos.org/a00104.html
Android	2008	11	Java + Kotlin (Android SDK and Android Studio)	Apache 2.0	http://source.android.com
Apache Mynewt	2016	1.3.x	C/Go	Apache 2.0	https://github.com/apache/mynewt-core
ARM Mbed	2009	5.15.x	C/C++	Apache 2.0	https://github.com/ARMmbed/mbed-os
Contiki/ Contiking	2002	4.x	C	BSD 3-Clause	https://github.com/contiki-ng
Huawei LiteOS	2013-2018	2.x	C	BSD 3-Clause	https://github.com/LiteOS
Linux/ Yocto	2010	3.1	Multiples	Multiples (GPL, LGPL, etc.)	http://yoctoproject.org
RIOT	2012	RIOT-2020.10	C/C++	LGPLv2.1	https://github.com/RIOT-OS/RIOT
Zephyr	2016	2.4.X	C (Developer Kit)	Apache 2.0	https://github.com/zephyrproject-rtos/zephyr

Nom de l'OS	Principales architectures supportées	Ressources demandées	Fonctionnalités remarquables
(Amazon) FreeRTOS	ARM, x86	4 Ko RAM	Intégration AWS pour la version Amazon
Android	x86, ARM	2 Go RAM	Toutes ou presque !
Apache Mynewt		16 Ko RAM	BLE 4.2
ARM Mbed	ARM Cortex-M	64 Ko RAM	BLE 4.2
SSL/TLS (Mbed TLS ou WolfSSL)	2002	4.x	C
Noyau préemp-tif	2013-2018	2.x	C
Contiki/ Contiking	ARM Cortex -M, MSP430	10 Ko RAM/100 Ko ROM	6LoWPAN, RPL, CoAP
Huawei LiteOS	ARM, RISC-V	10 Ko (noyau)	Support NB-IoT, Ethernet, Bluetooth, Wi-Fi, Zigbee
Linux/Yocto	Toutes ou presque !	32 Mo RAM	Toutes ou presque !
RIOT	Cortex-M, RISC-V, x86	1,5 Ko RAM, 5 Ko ROM	Noyau temps réel, support POSIX
Zephyr	ARM, RISC-V, x86	8 Ko RAM, 30 Ko ROM	Device tree support (DTS), Large set of protocol stacks

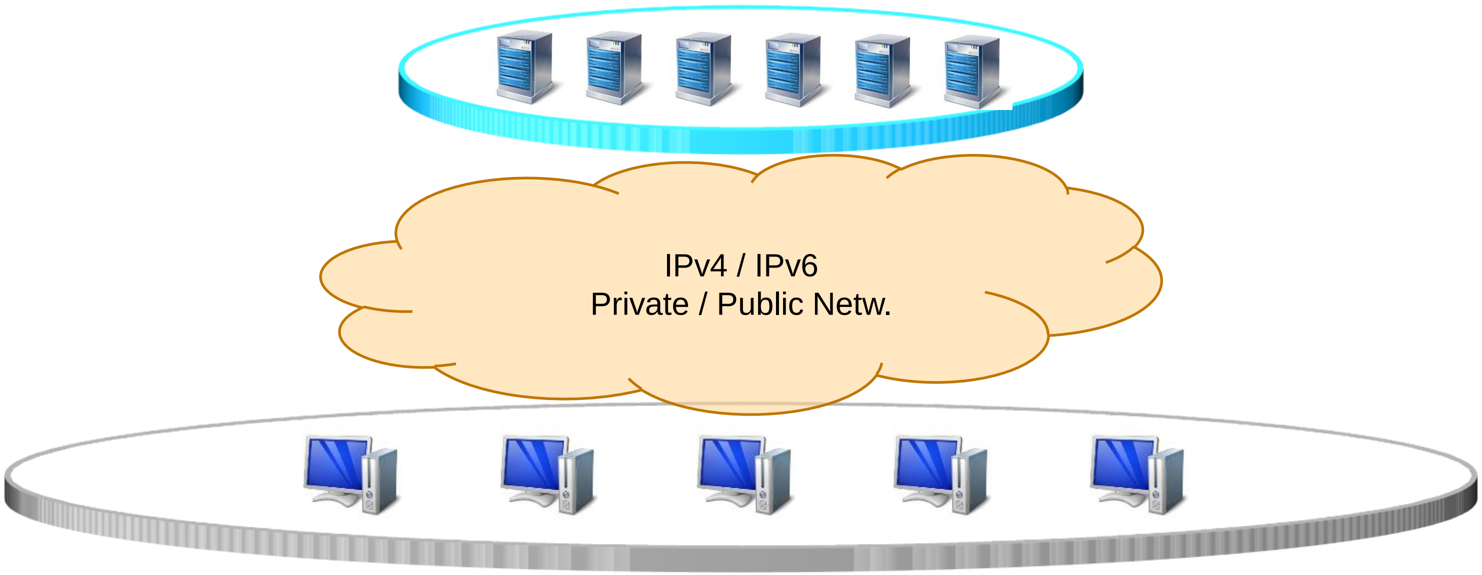
Source – Livre Blanc - L'open source pour l'IoT 2021 - À l'ère du edge computing - Pierre Ficheux, Frédéric Desbiens, Jonathan Rivalan

- **Amazon Alexa Home Skills API**
- **Wink API**
- **Caret API**
- **Ubidots API**
- **Apple HomeKit**
- **Unofficial Tesla Model S API**
- **Home Assistant API**
- **Withings API**
- **Google Assistant API**
- **Garmin Health API**
- **…**

- Smart Office
  - Room occupancy,
  - temperature,
  - humidity
  - …
  - Smart meeting room
  - Smart copier/scanner
  - Elevator system
  - Coffee machine
  - Doors and windows
  - …
- Smart Farm
- Smart City
- Smart Highway
- Smart Home
- …

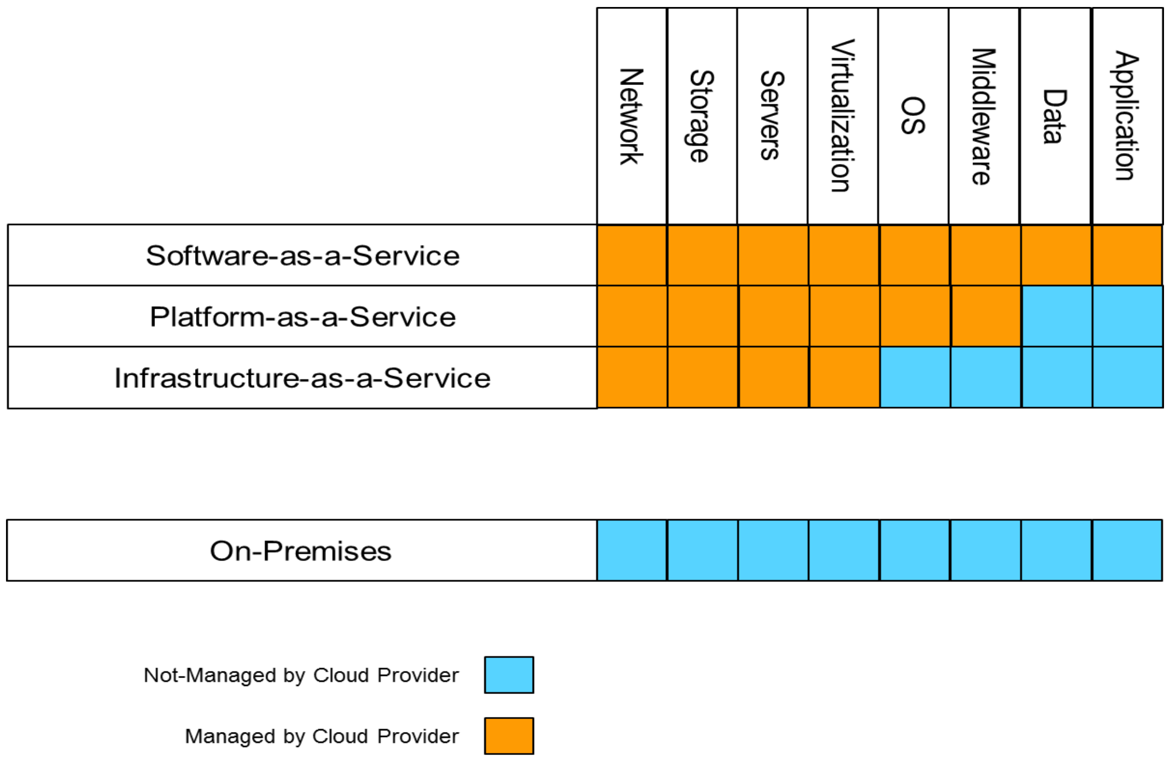
IoT architecture

IoT architecture: Cloud Computing

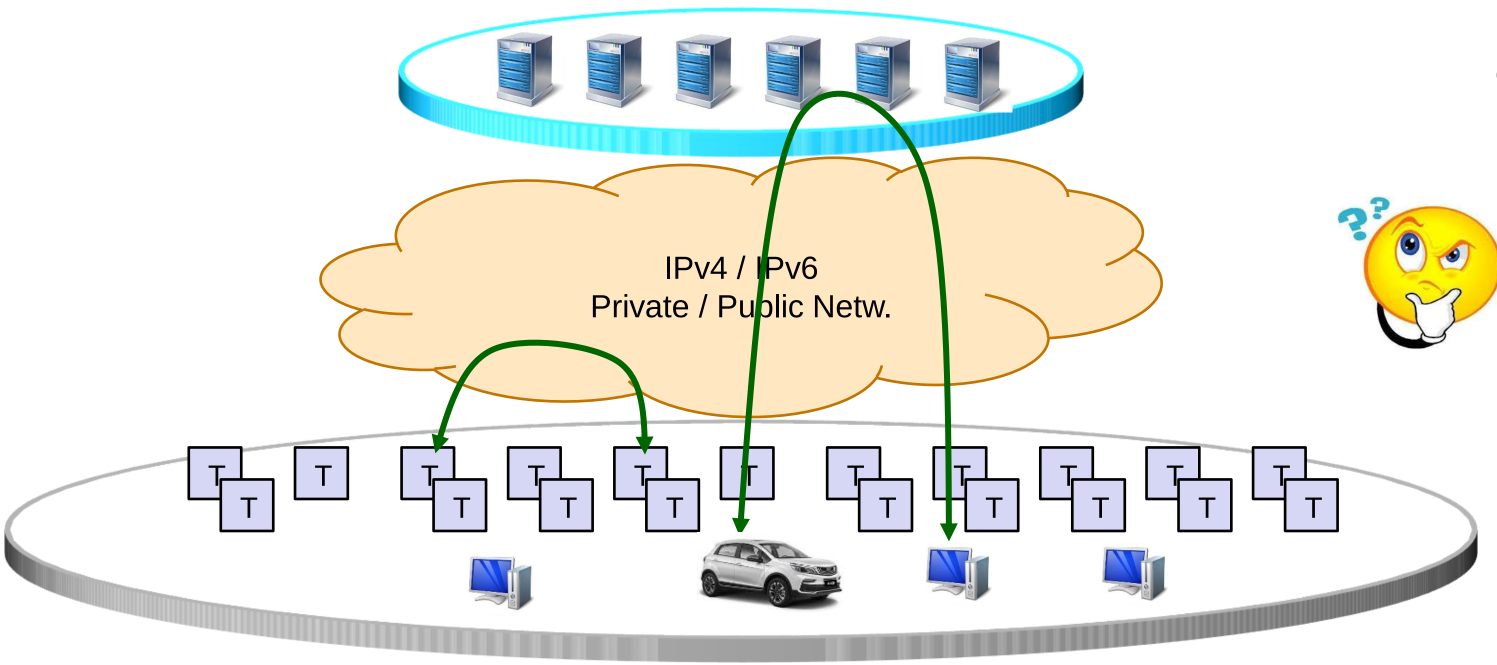


Cloud

- Cloud Computing
  - Already famous … necessary to define?
  - AWS “The on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.”



IoT architecture: Cloud Computing

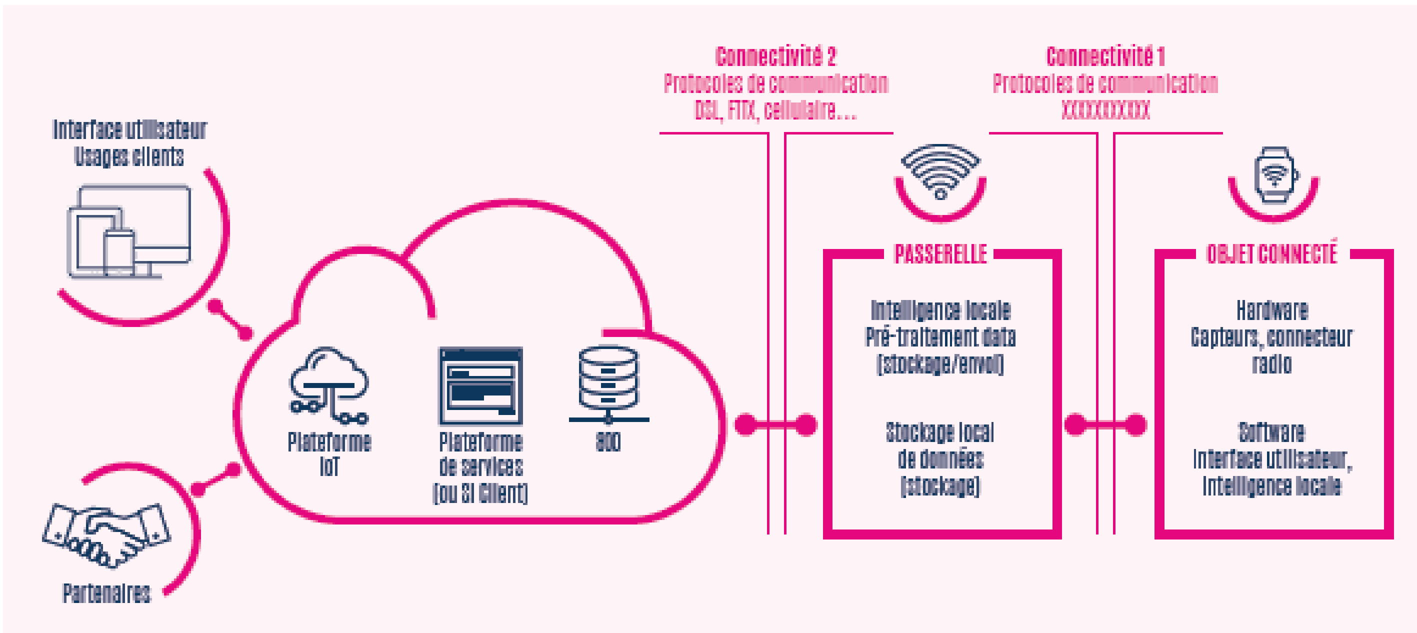


IoT architecture: Edge/Fog Computing

- Cloud Computing is not sufficient
  - Latency
  - Geographical Distribution
  - Mobility of end devices
  - Large number of “things”
  - Huge amount of data to process
  - Sensitive data
  - M2M communication
  - …
- Need of computing at the Edge closer to the things
- Fog Computing
  - OpenFog Consortium: Cisco, Intel, Microsoft, Princeton Univ., …
  - Fog networking, Fogging,…
  - Computing, storage and network away from the cloud as close to the endpoint as possible
  - computing resources and application services distributed via decentralized computing infrastructure.
- Edge Computing or Fog Computing
  - Just a location issue …
- Business model of Edge and Fog Computing to clarified

IoT architecture: Edge/Fog Computing

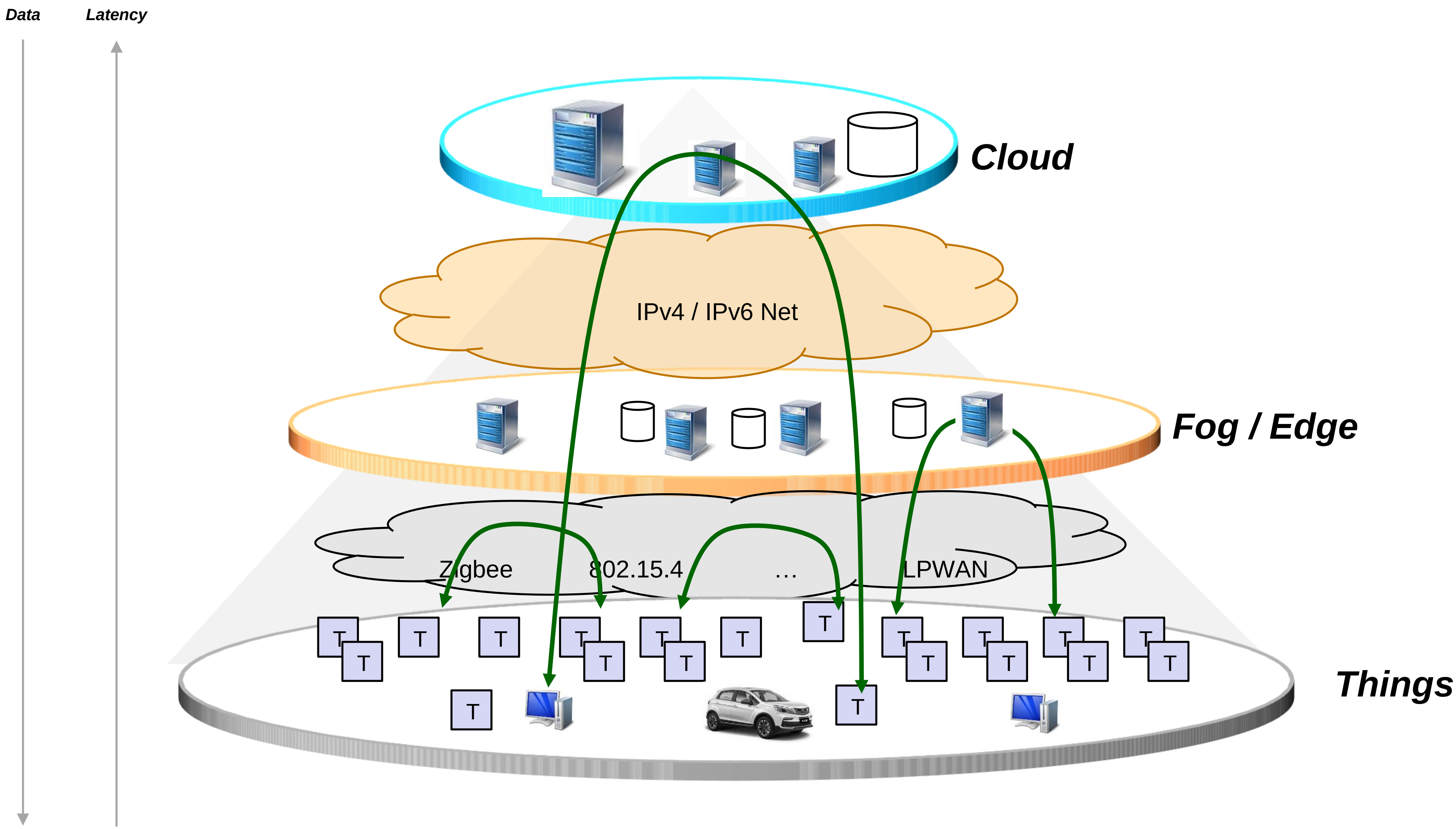
- Intermediate layer processing layer between things and backend (Cloud)
- M2M enabler
- Security Mgmt.
- Data Mgmt.
  - Basics analytics
  - Pre-process
  - Filter (unnecessary data unforwarded to things)
  - cache,
  - Storage
  - Computing off-load
  - buffering,
  - Optimisation
  - Pre-fetch (Cloud to Edge)
- Expected results
  - Bandwidth reduction
  - Latency reduction
  - Real-Time processing
  - More responsive
  - Better scalability
  - Conserve Netw. & Comp. resources
- AWS IoT Greengrass, Microsoft Azure IoT Edge, …



Architecture IoT

Source – Livre Blanc - L’open source pour l’IoT 2021 - À l’ère du edge computing - Pierre Ficheux, Frédéric Desbiens, Jonathan Rivalan

IoT architecture: Edge/Fog Computing

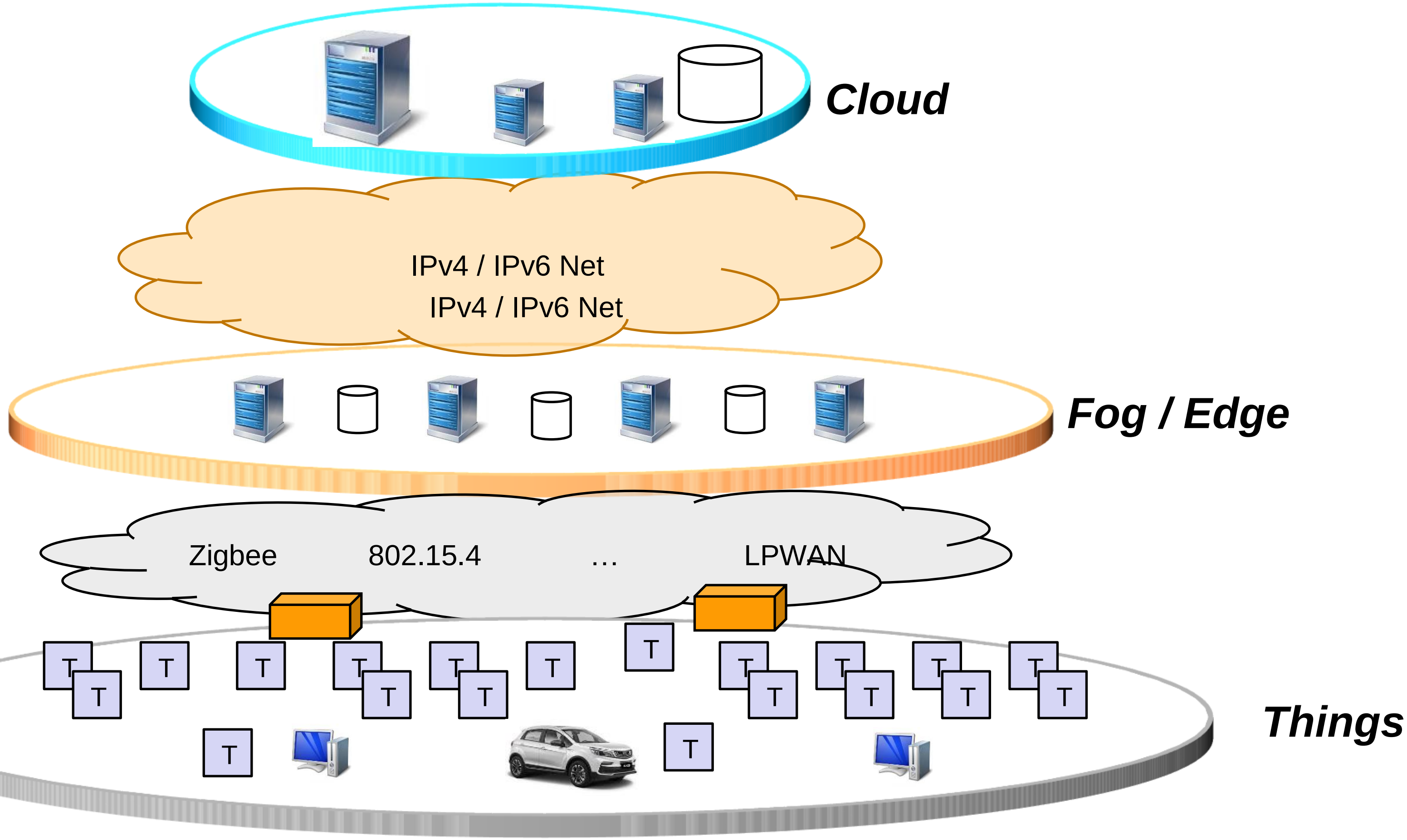


IoT architecture: enterprise/industrial environment

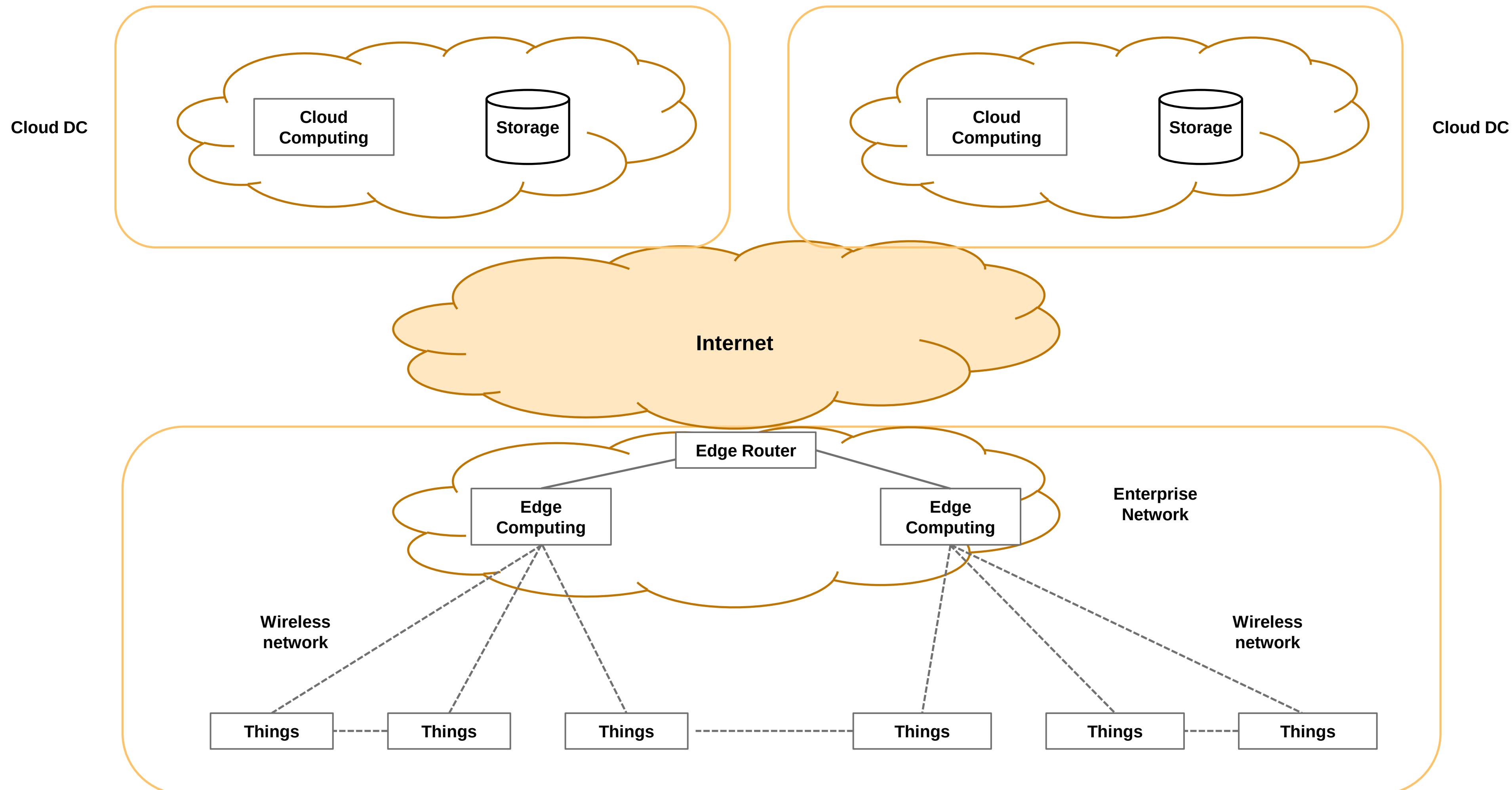
- Data analytics
- Cntral control
- Central processing
- …

- Real Time processing
- M2M control
- Caching
- Data analytics / Data viz
- …

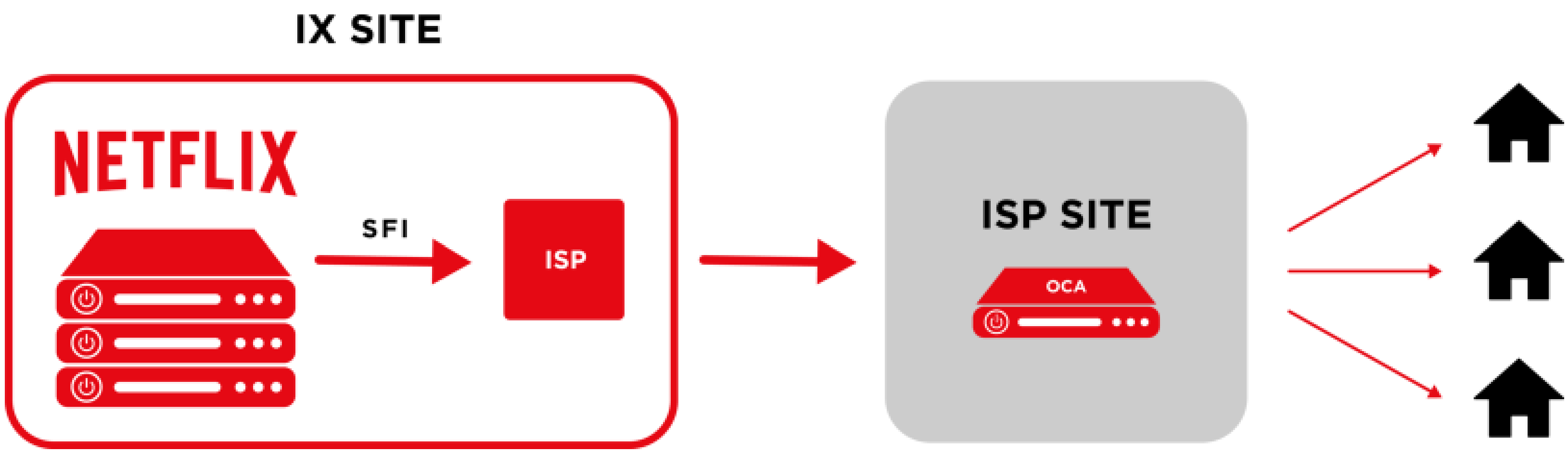
- Edge Gateway



IoT architecture: enterprise/industrial environment



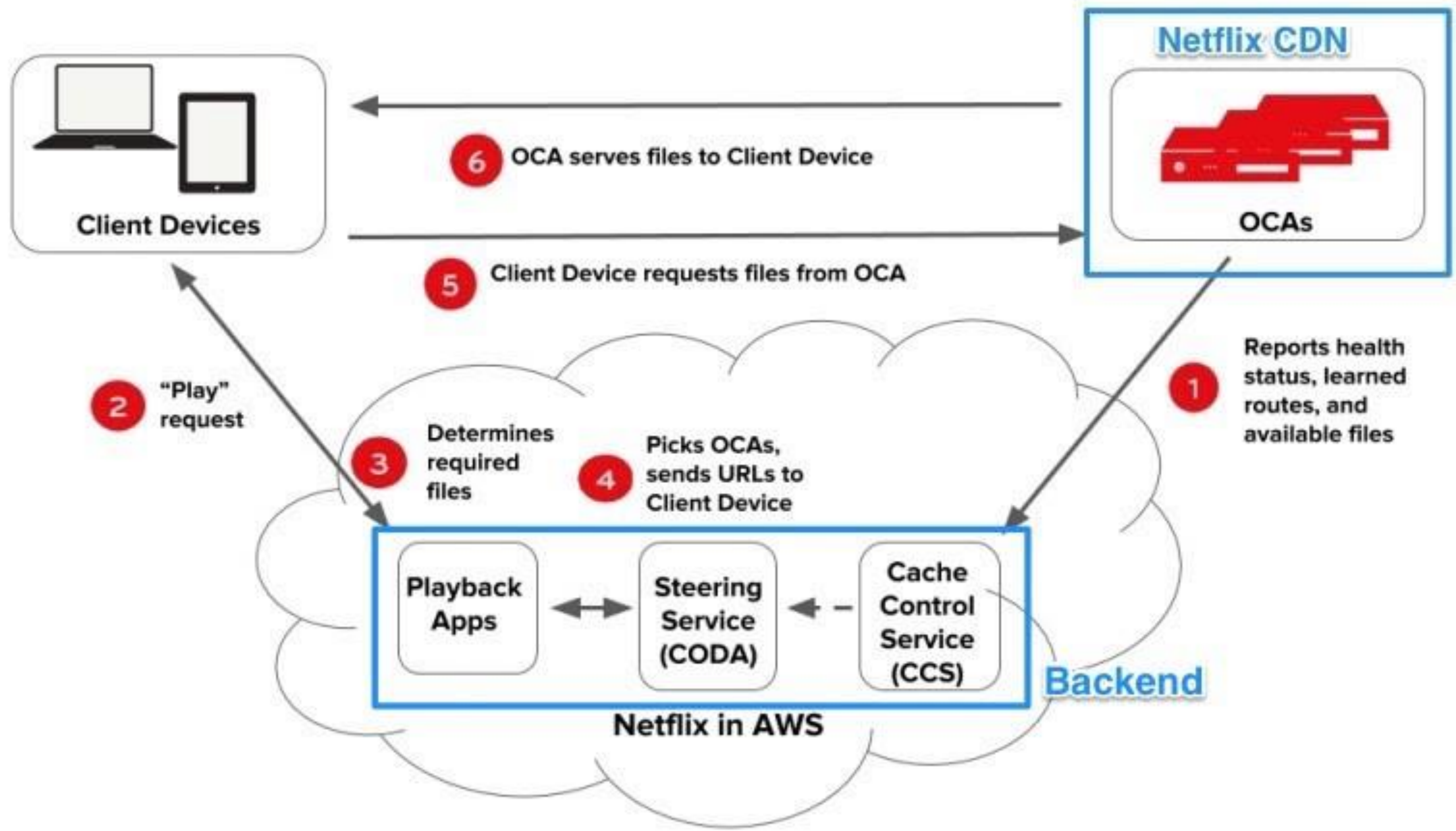
IoT architecture: e.g. Netflix content Delivery



IX – Internet Exchange Points
SFI – Settlement Free Peering
OCA – Open Content Appliance

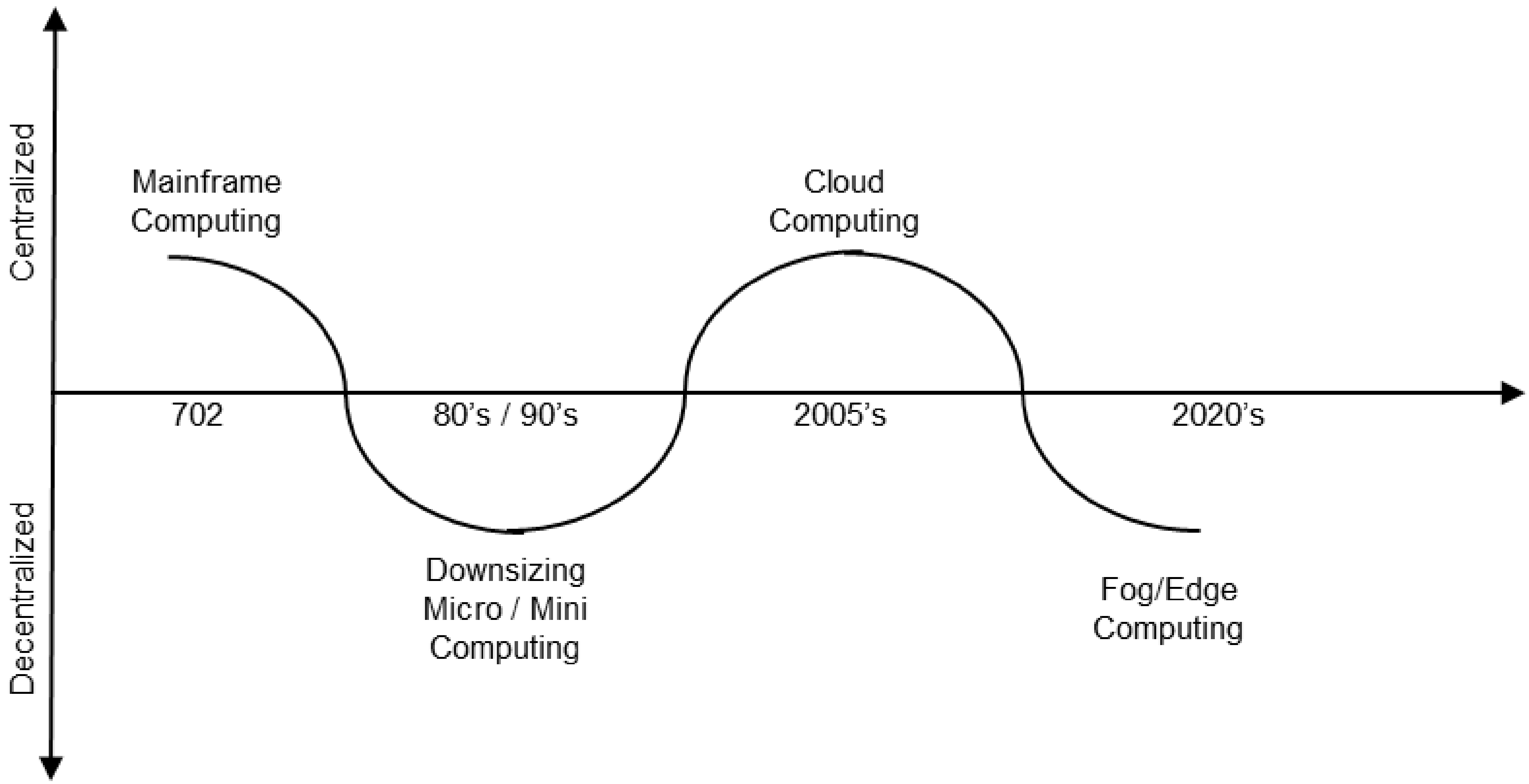
Source – A Design Analysis of Cloud-based Microservices Architecture at Netflix, Cao Duc Nguyen

IoT architecture: e.g. Netflix content Delivery



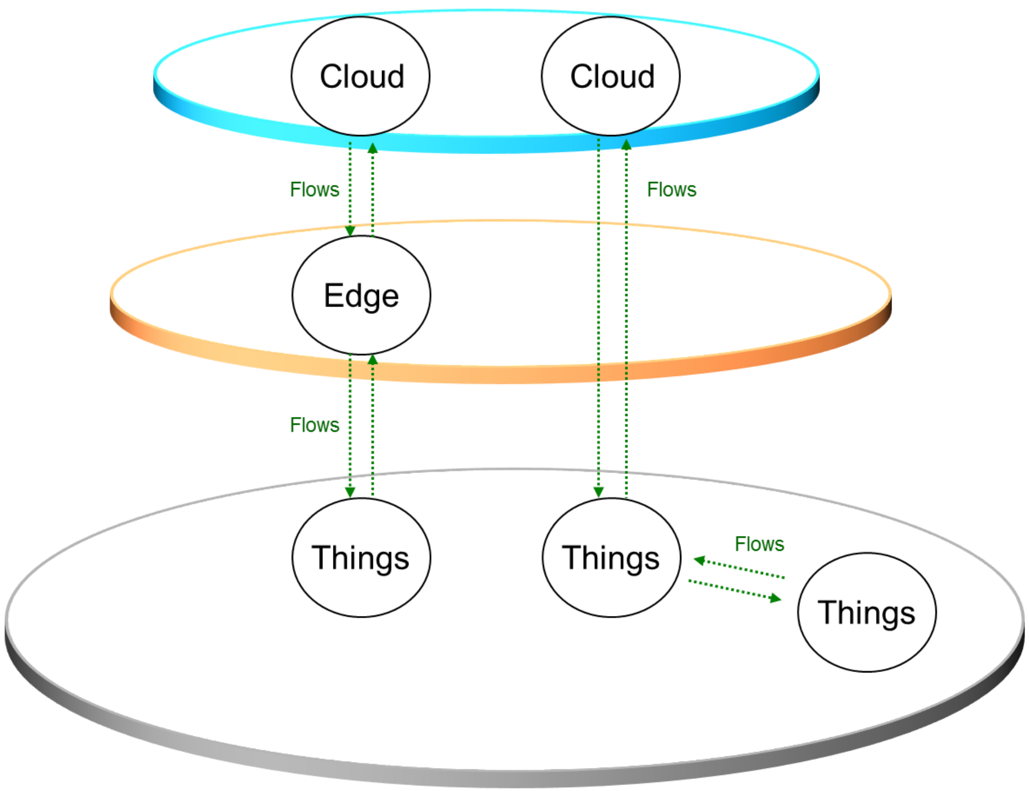
Source – A Design Analysis of Cloud-based Microservices Architecture at Netflix, Cao Duc Nguyen

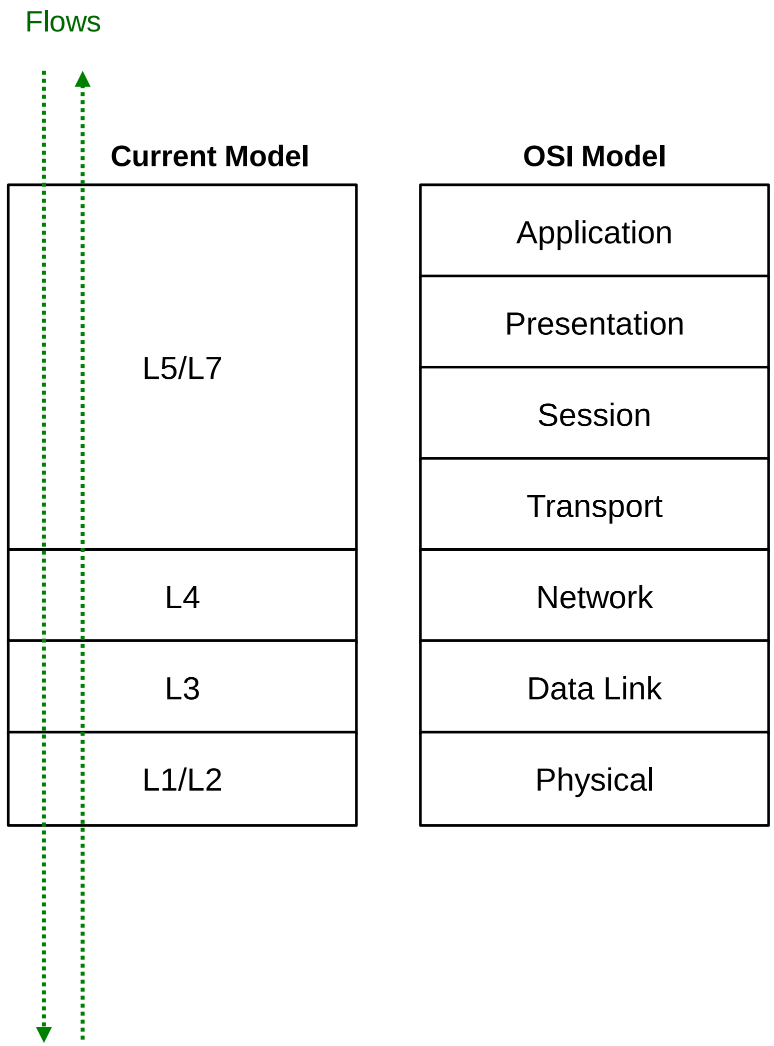
IoT architecture: Edge/Fog Computing



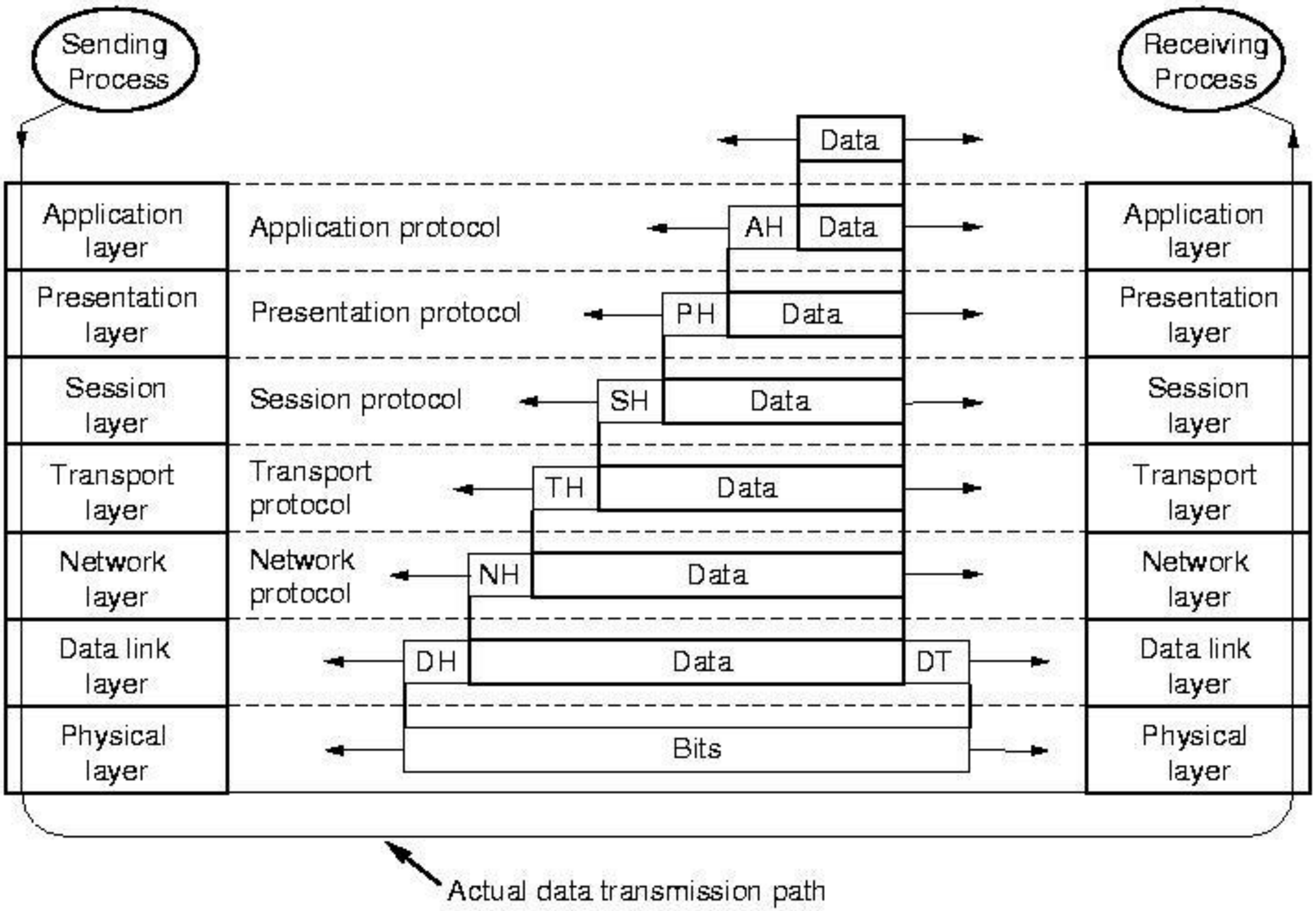
Connectivity
&
Protocols

IoT information flows

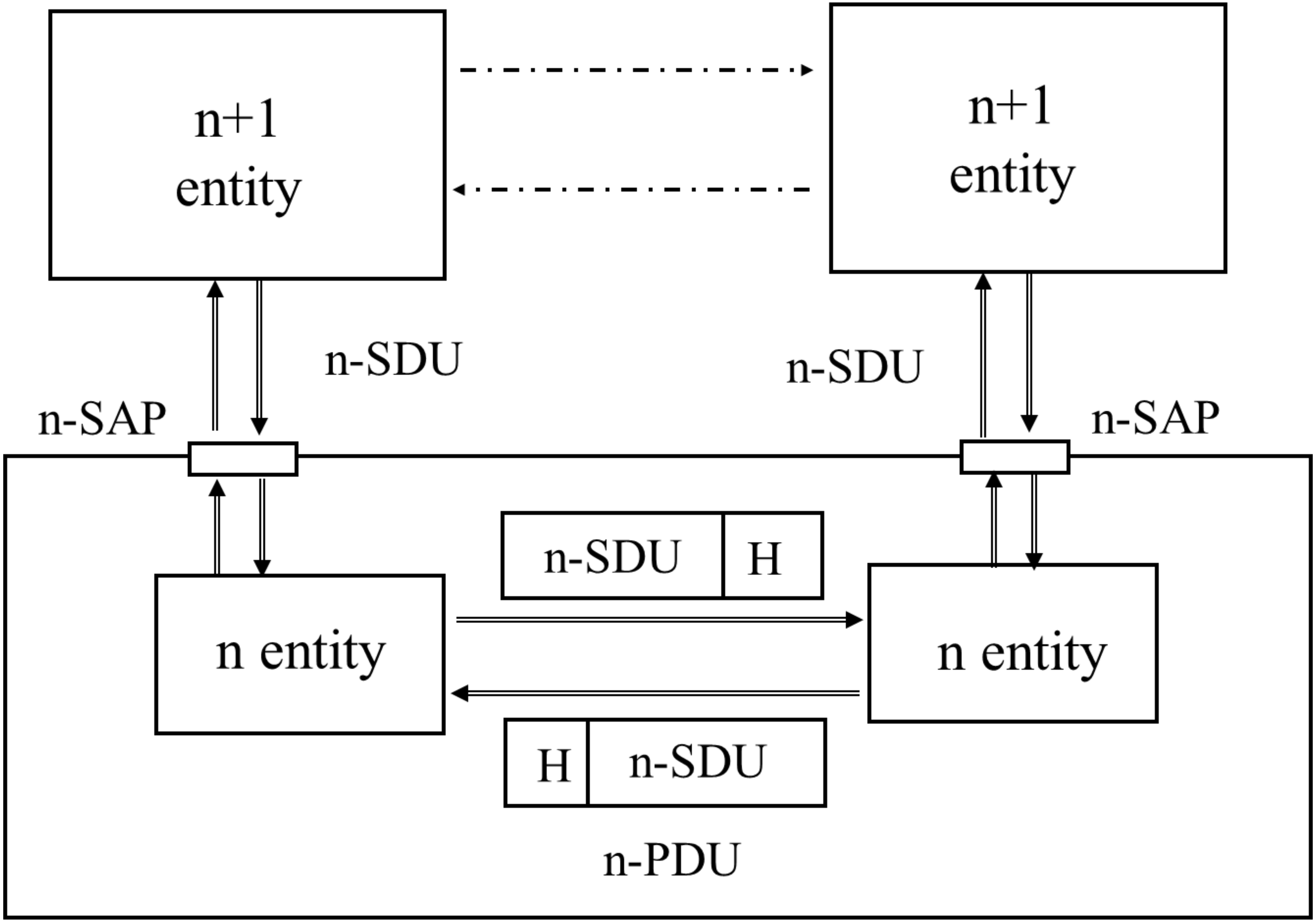




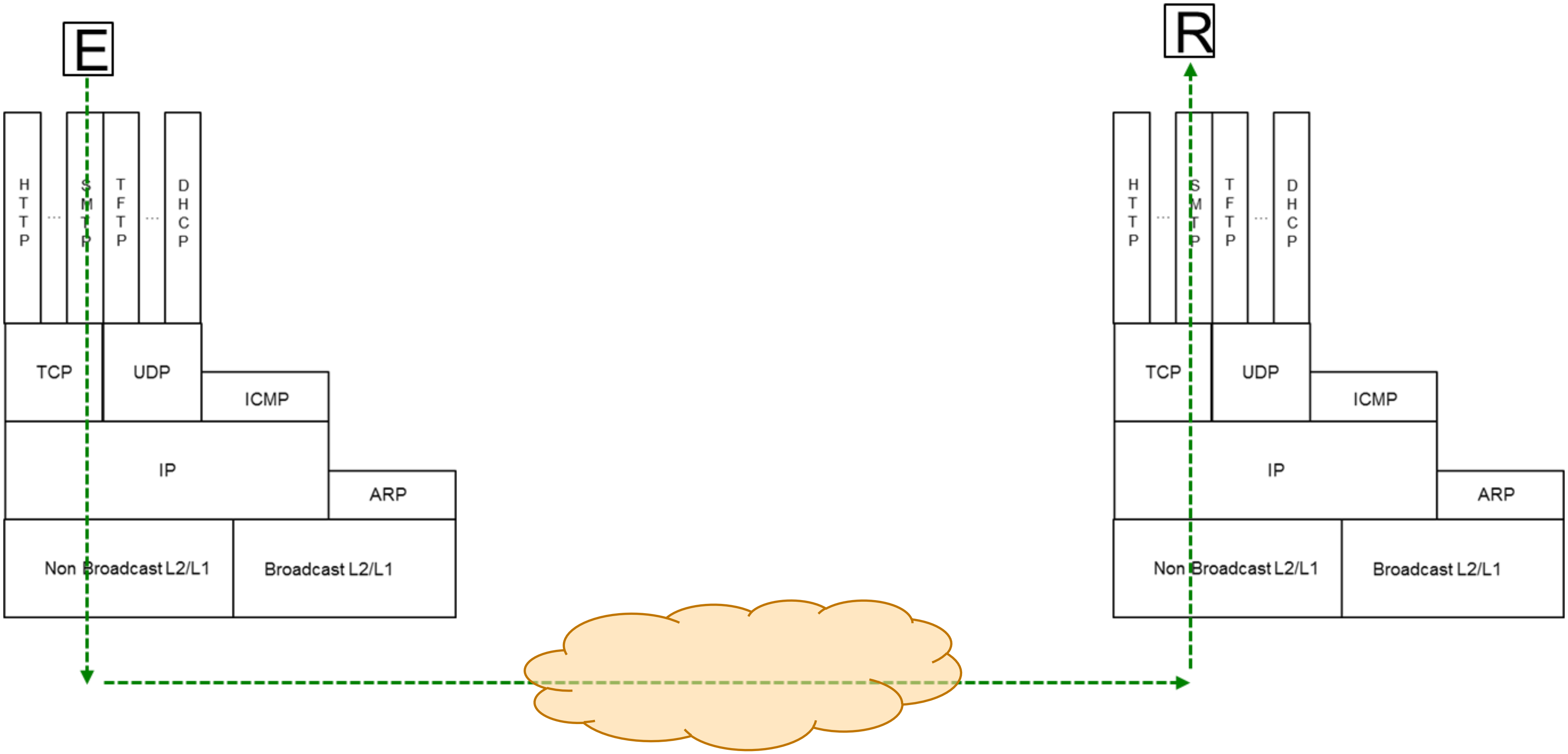
Encapsulation / de encapsulation principle (reminder)



Layering principle (reminder)

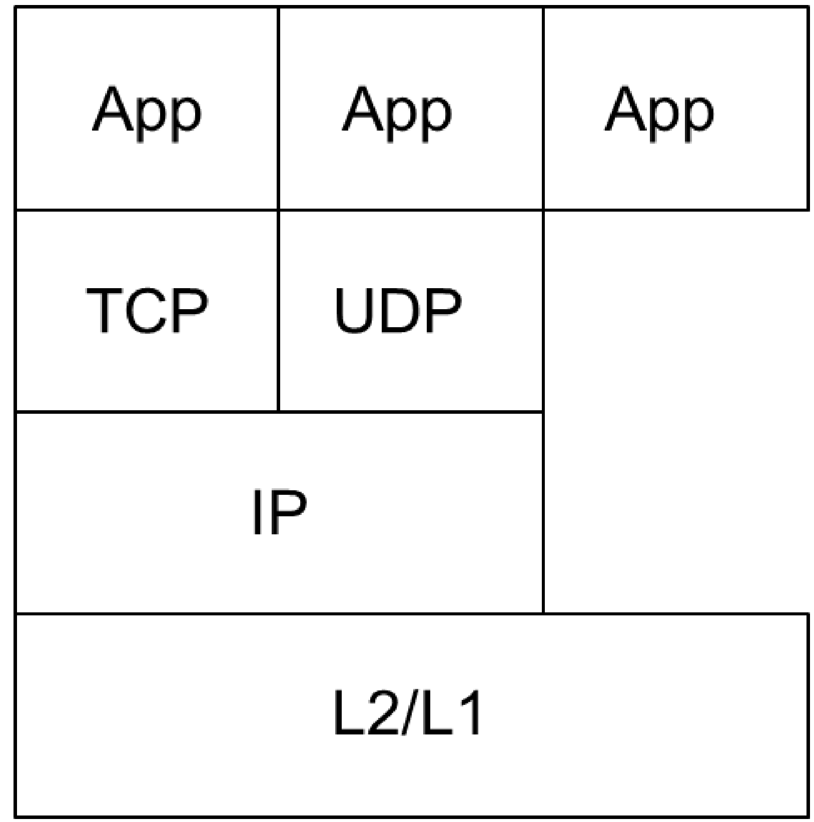


TCP/IP: THE current 4-layers model (reminder)

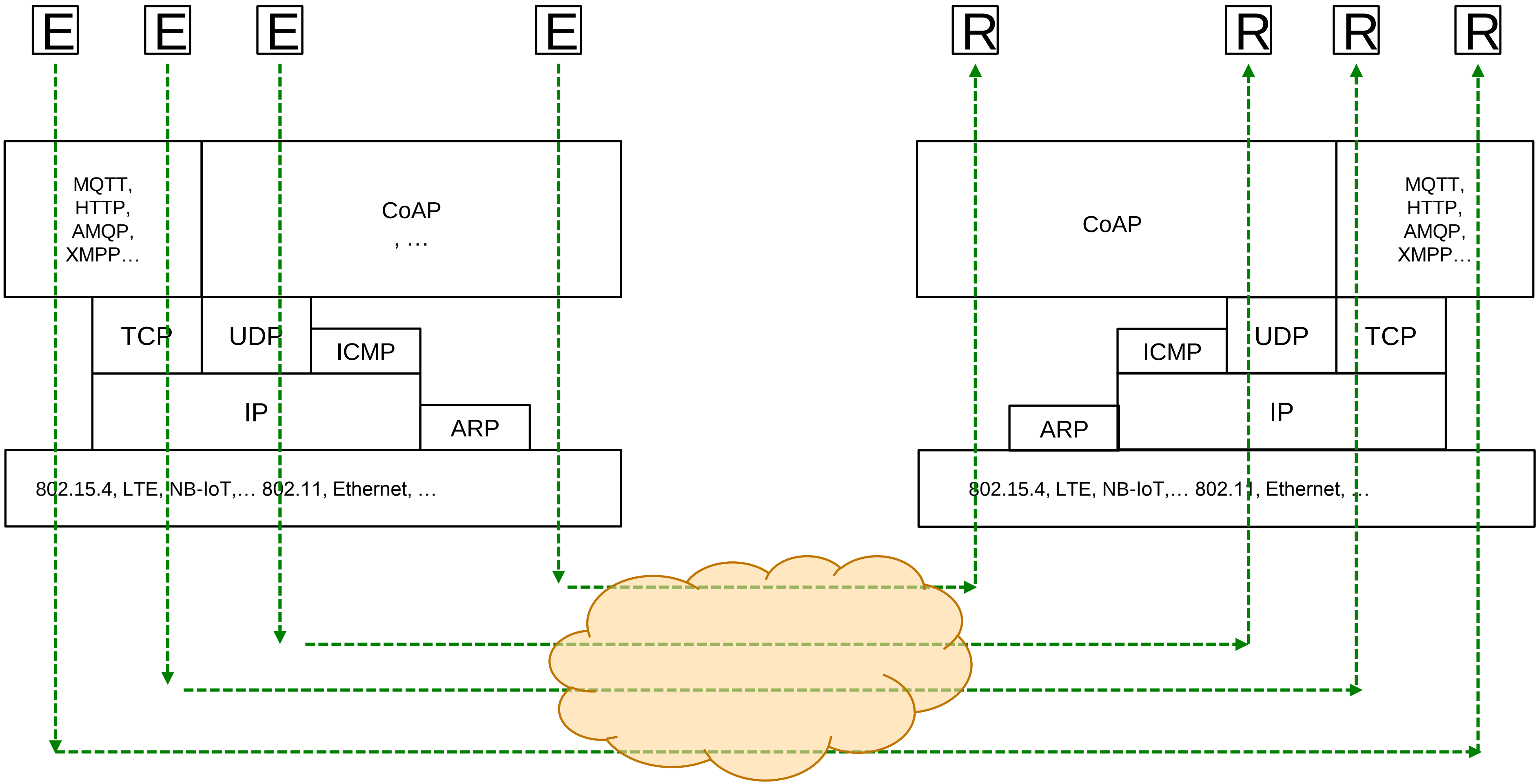


IoT: stack of protocols

- L5/L7 IoT protocols
  - MQTT, CoAP, AMQP, XMPP
  - LWM2M, DDS, SNMP, …
  - The winner will be???
- L4 IoT protocols
  - TCP, UDP
- L3 IoT protocols
  - IPv4, IPv6, 6LoWPAN, RPL,
- L1/L2 IoT technologies
  - A lot of competitors …
  - The winner will be???



IoT: stack of protocols



- IEEE
  - L1/L2 technologies
- ITU-T
- ANSI
- Proprietary
- …
- IETF / Internet
  - L3 / L4 / L5-L7
  - IAB / IETF (wg) / IRTF (wg)
  - Request For Comments (SRI-NIC) xxxx

IoT: connectivity competitors (L1/L2 mainly)

- Low-Power Wireless Area Network
- Short Range
  - RFID
  - NFC
  - BT / BLE
  - ZigBee
  - Z-Wave
  - IEEE 802.11
  - 802.15.4
- Long Range
  - LoRA
  - SigFox
  - LTE-M Cat 0
  - NB-IoT
- LiFi (?)

- Radio Frequency IDentification
- 1945
- Frequencies
  - LF: 125-134KHz
  - HF: 13.56MHz
  - UHF: 433MHz, and 860-915MHz
- Tags and tags readers
- Tags (Transponders)
  - Chip
  - Antenna
  - optional capabilities (memory, sensors, power)
  - Unique identification serial number (32 –64 –96 –128 ,...) Bits

- Memory type
  - TID (read only), EPC (Electronic Product Code) (read only), USER (r/w) et Reserved (security).
- Active / passive
  - Passive or non-battery powered RFID tag
  - Active or battery powered RFID tag
- Tag reader
  - Decoder & antenna
  - Sends pulse of energy and waits for response
  - Always on or only in response to external event

LF	30 kHz to 300 kHz	< 10 cm
HF	3 MHz to 30 MHz	< 1 m
UHF	300 MHz to 3 GHz	< 10 m

Antenna

Optional: memory, power, sensor

Chip

Reader

Transponder / Tag

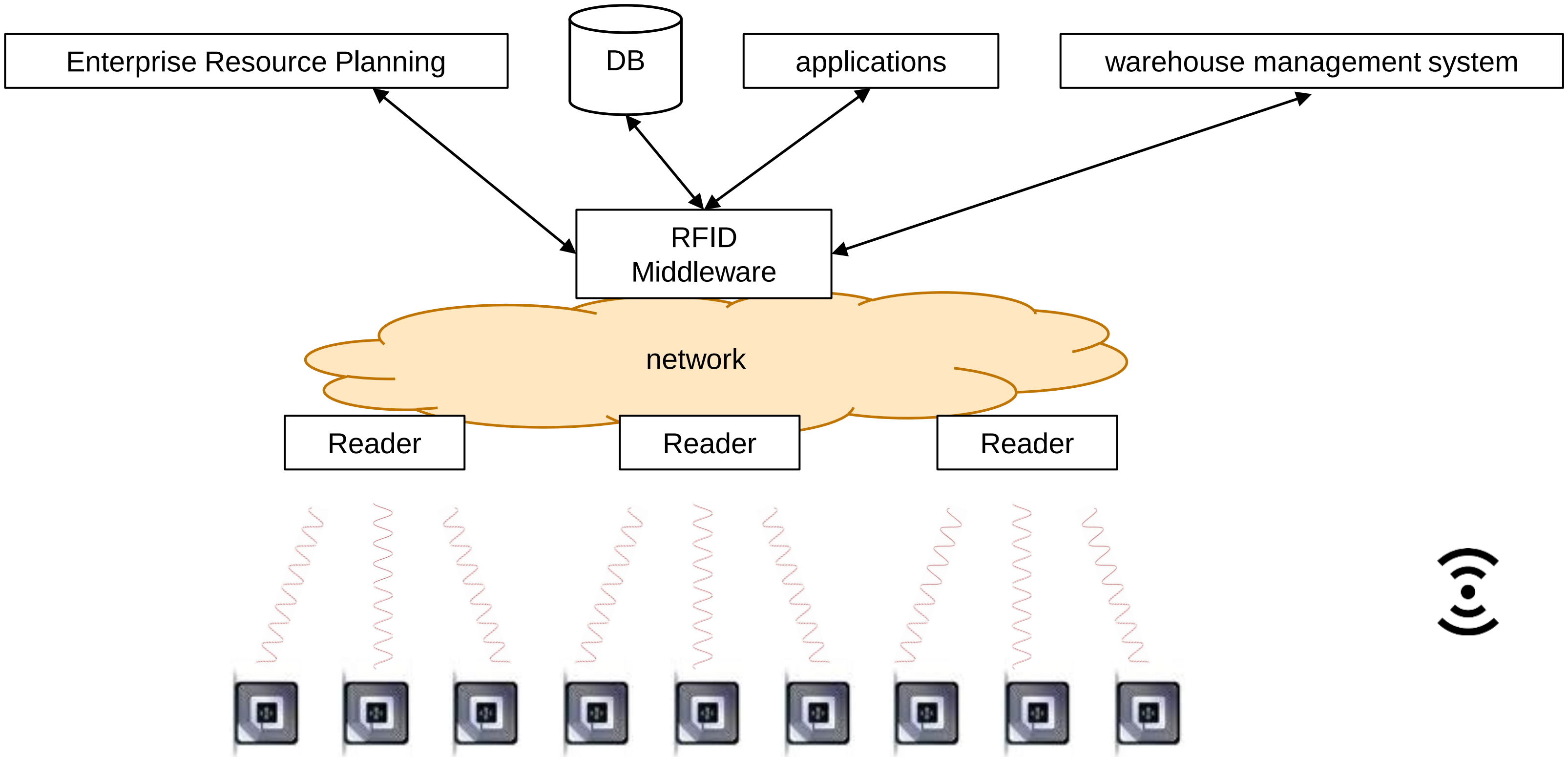
Electromagnetic field

Data

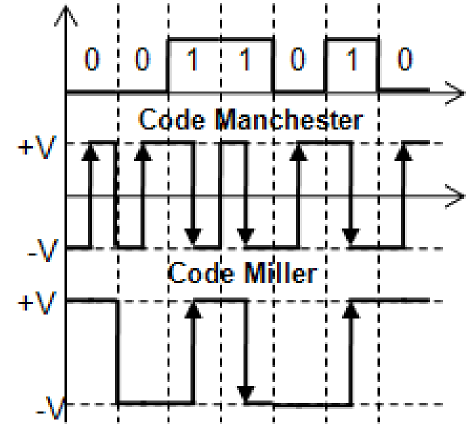
Active
Semi passive
Passive

Class 0 / Read only
Class I / Write once read only (worm ?)
Class II / Read Write
Class III / Read Write with on board sensor
Class IV / Read Write with integrated transmitter

- Contactless Card
  - ISO/IEC 14443 / 13,56 MHz (ISM)
- Smart Tag
- …



- Near-Field Communication
- ISO/IEC 18000-3
  - ISO/IEC14443 extension
- RFID offshoot
  - NFC is designed for use by devices close to each other
  - RFID vs NFC: Just a question of range thus usages
- Characteristics
  - Range ~10cm
  - 13.56MHz, with a bandwidth 14kHz.
  - data rates: 106, 212 and 424 Kbits/s
  - Modified Miller Coding or Manchester coding



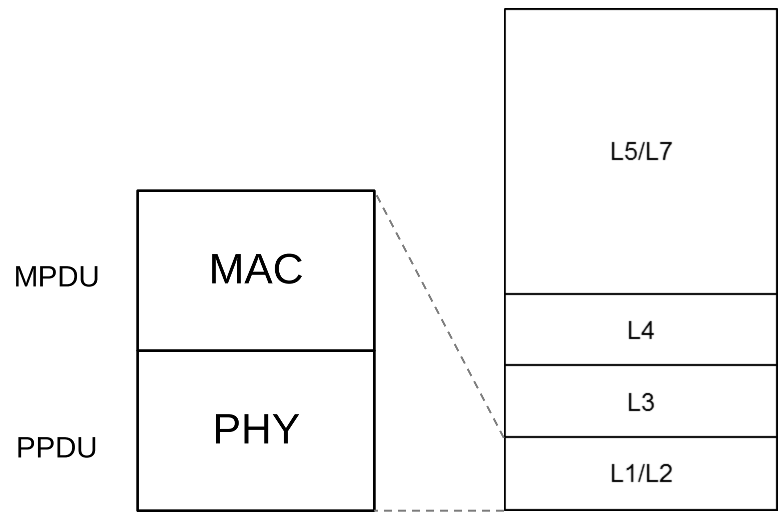
- Usage
  - e.g., Smartphones contactless payments
- Electromagnetic induction between two loop antennas
- Share information < 4cm.
- Two communication modes
  - Passive communication mode: In this mode, only one NFC device generates an RF field. The second device referred to as the target uses a technique called load modulation to transfer the data back to the primary device/initiator
  - Active Communication mode: In this mode of communication, both NFC devices generate an RF signal on which the data is carried

Year	Event
1983	The first patent to be associated with RFID was granted to Charles Walton
2002	NXP Semiconductors and Sony co-invent NFC
2004	Nokia, Phillips and Sony established the NFC forum
2006	Initial specifications for NFC Forum Tags and "Smart Poster" records
2006	Nokia launches the first NFC phone (Nokia 6131)
2009	NFC Forum releases Peer-to-Peer standards
2010	Samsung, Nexus 5: First Android NFC phone shown
2010	AT&T, Verizon, T-Mobile announces Softcard mobile payment joint venture
2011	Google I/O "How to NFC" demonstrates NFC to initiates a game and to share a contact, URL, app, video, ...
2011	RIM is 1st company for its devices is certified by Mastercard worldwide, the functionality of PayPass
2012	Samsung introduces TecTile, a set of NFC stickers and a companion App for Android to read/write TecTile
2012	Sony introduces "Smart Tags" using NFC technology to chab=nge modes and profiles on Sony smart phone
2012	Wired US is the 1st mass market publication to feature NFC enable advertisements
2013	Samsung and Vise announces major partnership to develop mobile payments
2014	Apple introduces iPhone 6 with Apple Pay using NFC Tecnology

Source : NFC EE174 – SJSU - Tan Nguyen

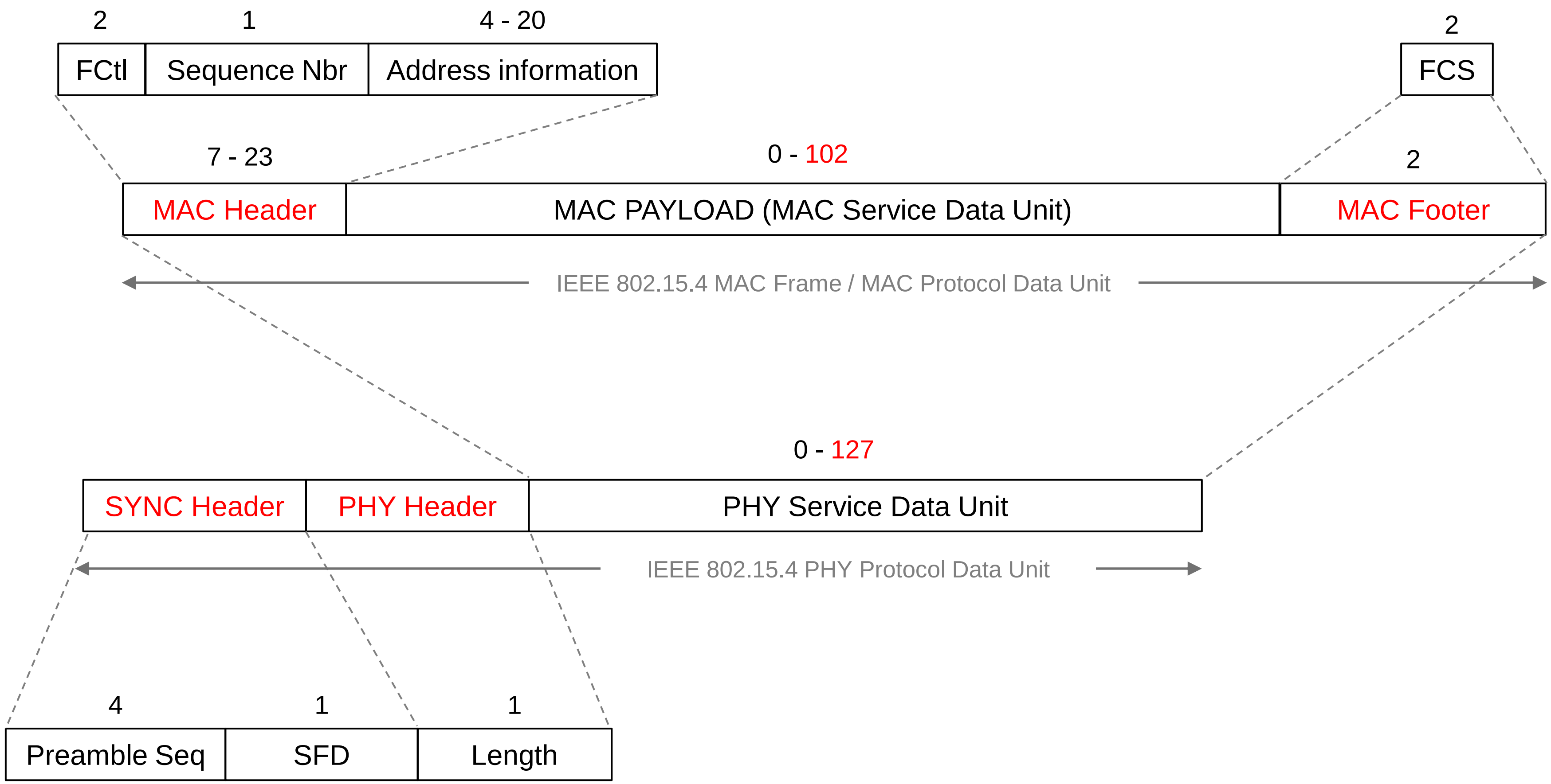
Animal Tag

- Belongs to the IEEE 802.15 family of protocols
  - 802.15.3 High Rate WPAN
  - 802.15.6 Body Area Networks
  - 802.15.7 Visible Light Communication
  - …
- Low-Rate Wireless Personal Area Network
- Protocol with acknowledgment
- Low Power oriented
- MAC
  - Non-beacon mode => CSMA/CA
  - Beacon mode
- PHY
  - 20 kpbs at 868 MHz / 3 channels / Europe
  - 40 kbps at 915 MHz / 10 Channels / US
  - 250 kbps at 2,4 GHz / 16 channels
  - MTU 127 Bytes
- MPDU / PPDU

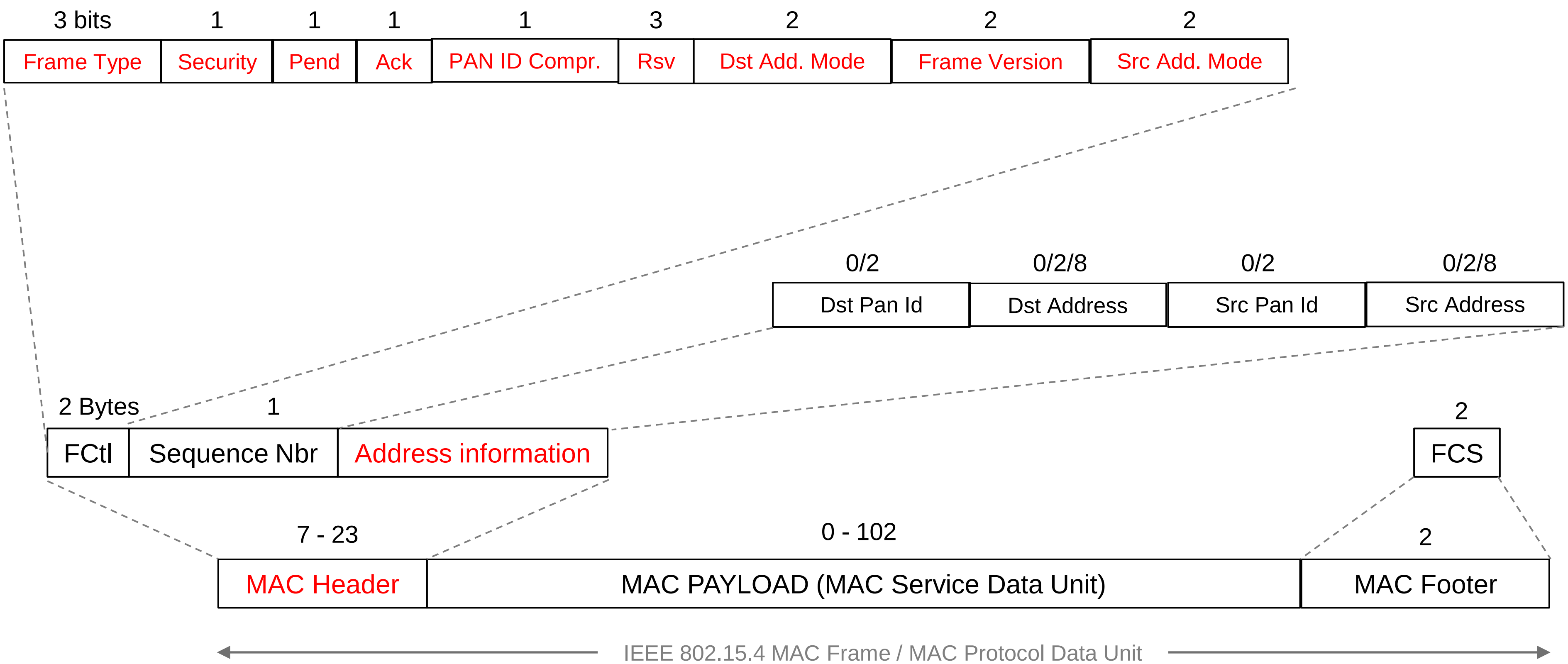


- PAN Coordinator
- Nodes
  - FFD
  - RFD
- Full Function Device
  - PAN Coordinator
  - Router
  - End system
  - FFD ⇔ FFD
  - FFD ⇔ RFD
- Reduced Function Device
  - End System only
  - RFD ⇔ FFD
- Topology
  - Star
  - Mesh
  - Cluster
- Association procedure
  - association request frame / association response
- Frame type
  - Data Frame
  - Beacon Frame
  - Acknowledgment Frame
  - MAC Command Frame

802.15.4: frame format



802.15.4: frame format



- Frame Type
  - 000 Beacon
  - 001 Data
  - 010 Ack
  - 011 MAC Command
  - 100 – 11 reserved
- Security
  - 1 protected by MAC sublayer (Security header field of the MHR) / 0 not protected
- Pending
  - 1 more data for the recipient (Beacon Frame) / 0 no more data
- Ack
  - 1 acknowledgment irequired from the recipient device
- PAN ID Compression

802.15.4: ACK frame format

2	1	2
FCtl	Sequence Nbr	FCS

4	1	1	
Preamble Seq	SFD	Length	PHY Service Data Unit

802.15.4: adresses

- EUI64
- 16-Bit PAN ID

0/2	0/2/8	0/2	0/2/8
Dst Pan Id	Dst Address	Src Pan Id	Src Address

I/G	U/L	Organizationally Unique ID	Manufacturer assigned
1	1	22	40

0 = Individual (unicast) / 1 = Group (multicast/ broadcast)
0 = Universal (IEEE) / 1 = Local (Private)

MAC (EUI-48)

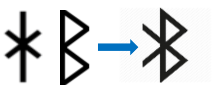
I/G	U/L	Organizationally Unique ID	Manufacturer assigned
1	1	22	24

e.g. 0x02608C4AFFE8

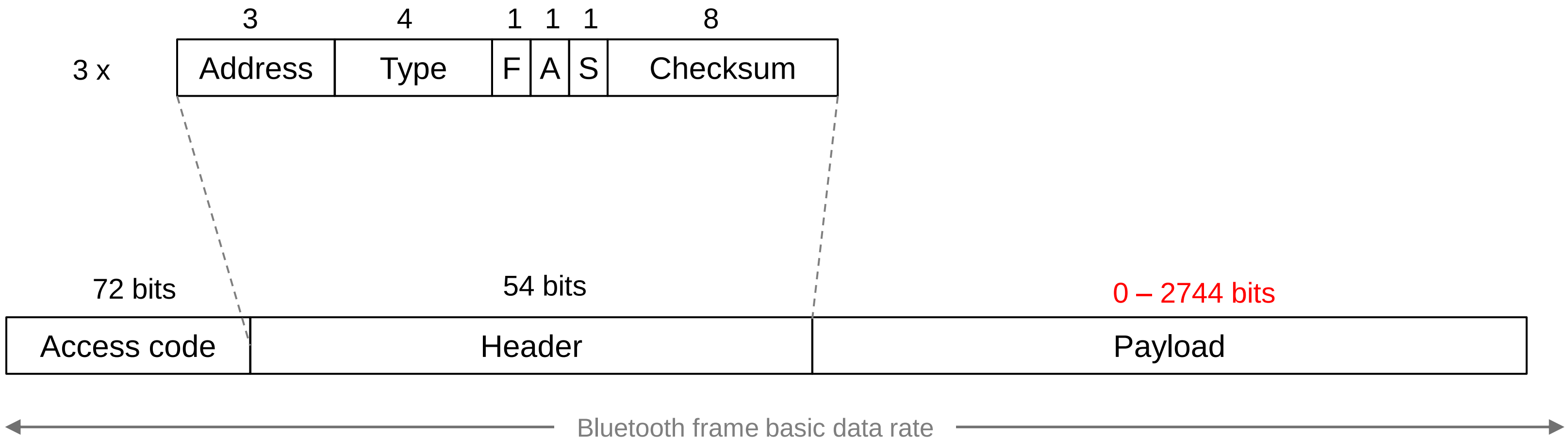
02608C => 00000010

- IEEE 802.15.4
  - 2003 release. This was the initial release of the IEEE 802.15.4 standard. It provided for two different PHYs - one for the lower frequency bands of 868 and 915 MHz, and the other for 2.4 GHz.
  - 2006 release. This 2006 release of the IEEE 802.15.4 standard provided for an increase in the data rate achievable on the lower frequency bands. This release of the standard updated the PHY for 868 and 915 MHz. It also defined four new modulation schemes that could be used - three for the lower frequency bands, and one for 2.4 GHz.
- IEEE 802.15.4a
  - This version of the IEEE 802.15.4 standard defined two new PHYs. One used UWB technology and the other provided for using chirp spread spectrum at 2.4 GHz.
- IEEE 802.15.4c
  - Updates for 2.4 GHz, 868 MHz and 915 MHz, UWB and the China 779-787 MHz band.
- IEEE 802.15.4d
  - 2.4 GHz, 868 MHz, 915 MHz and Japanese 950 - 956 MHz band.
- IEEE 802.15.4e
  - This release defines MAC enhancements to IEEE 802.15.4 in support of the ISA SP100.11a application.
- IEEE 802.15.4f
  - This will define new PHYs for UWB, 2.4 GHz band and also 433 MHz
- IEEE 802.15.4g
  - This will define new PHYs for smart neighborhood networks. These may include applications such as smart grid applications for the energy industry. It may include the 902 - 928 MHz band.
- 802.15.4z-2020
  - IEEE Standard for Low-Rate Wireless Networks--Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques

- Bluetooth
- Harald Blaatand (908 - 986)
- le Bluetooth Special Interest Group (SIG)
  - 1998
  - Ericsson, IBM, Intel, Nokia, Toshiba



- IEEE 802.15.1
- Radio network
- UHF / 2,4 GHz
- ~10/20 m
- 1.0 May 1999 => 5.2 December 2019
- Architecture
  - Piconet
  - Scatternet

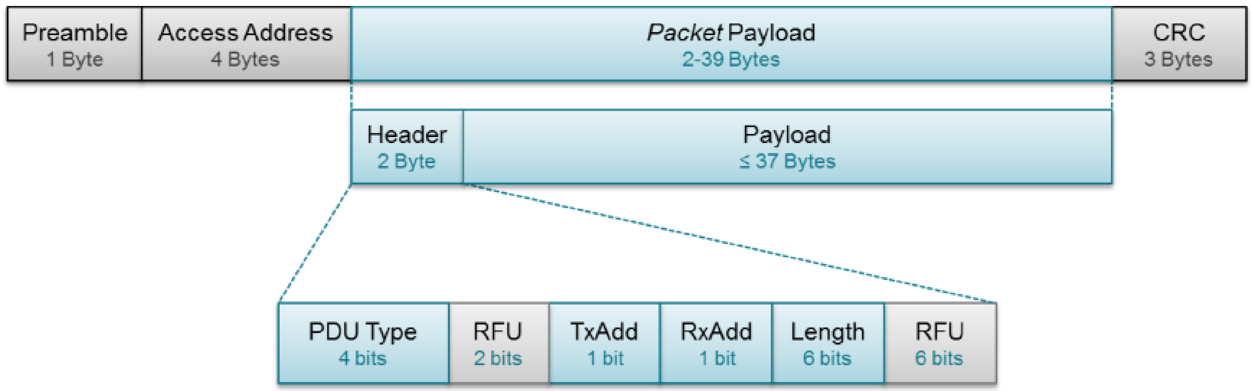


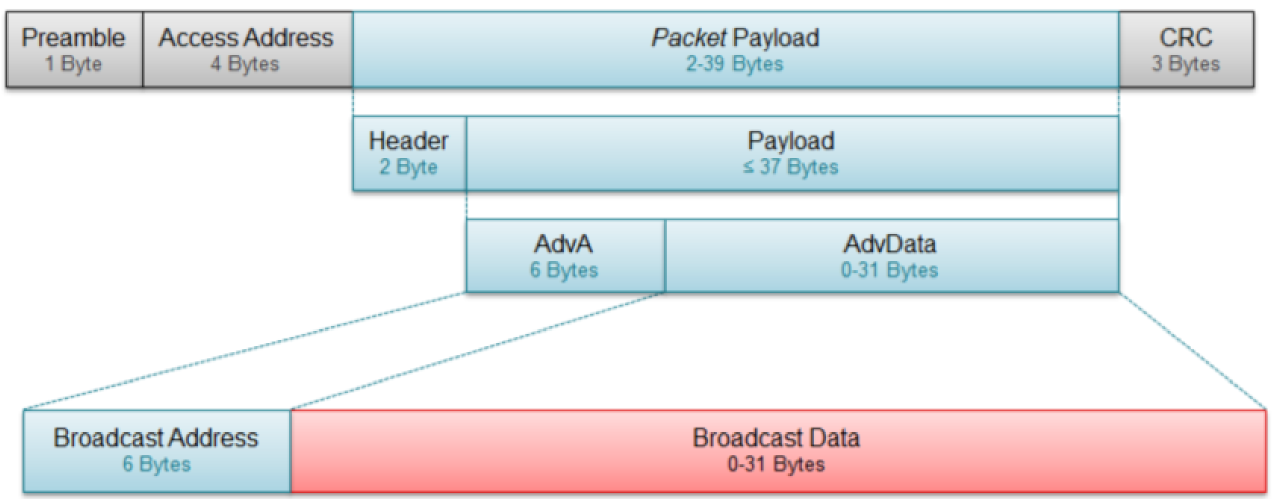
• Access code	synchronization to identify the master
• Address	identify a maximum of seven slaves numbered 1 to 7. An address 0 depicts broadcast.
• Type	identifies data from upper layers. It identifies whether the frame is ACL, SCO, poll or null.
• F	bit for flow control. When the device cannot receive more frames, F is set to 1.
• A	bit for acknowledgement, for piggybacking an ACK to the end of the frame.
• S	denote sequence number of the frame for detect retransmission. Only a single bit suffices since stop and wait protocol is used.
• Checksum	An 8-bit field containing checksum for error detection.

- Bluetooth Low Energy
  - Smart Bluetooth
  - Based on IEEE 802.15.1

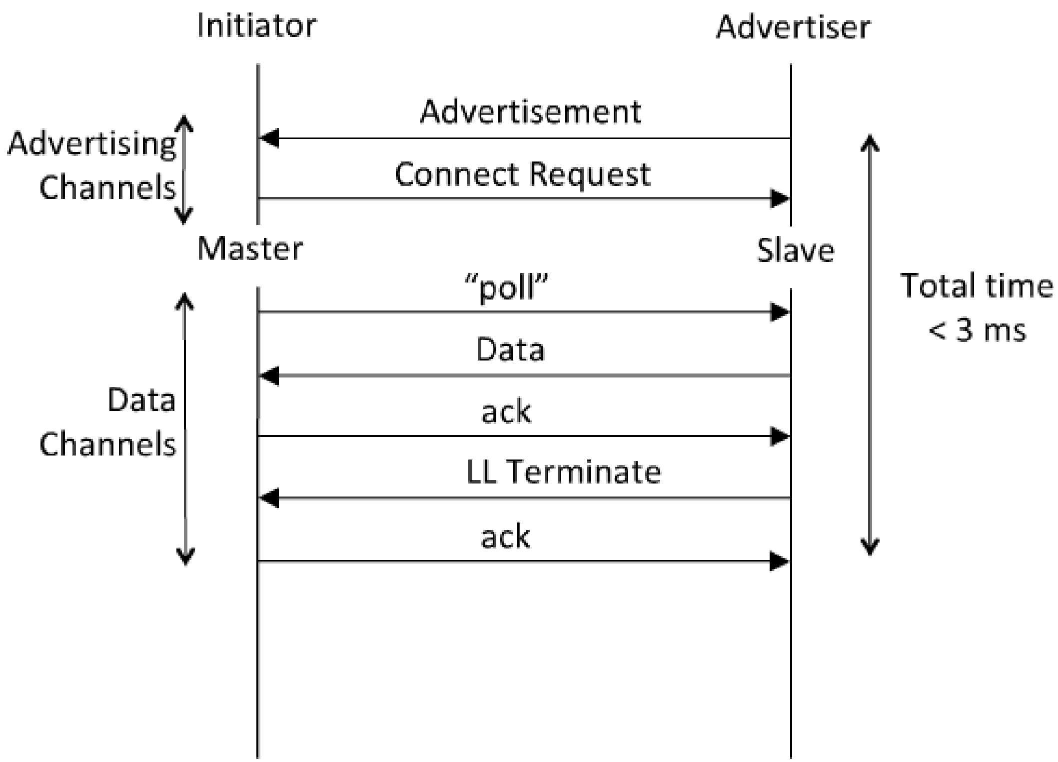
	« classic » bluetooth	BLE
Rate	1-3 Mbps	1 Mbps
Range	~10 m	~> 100 m (?)
Frequency	2,4 GHz	2,4 Ghz
Latency	100 ms	6 ms
Voice support	Yes	No
Topology	Star	Star
Power consumption	~1 W	~0,01 W => 0,5 W

BLE: Data packet format

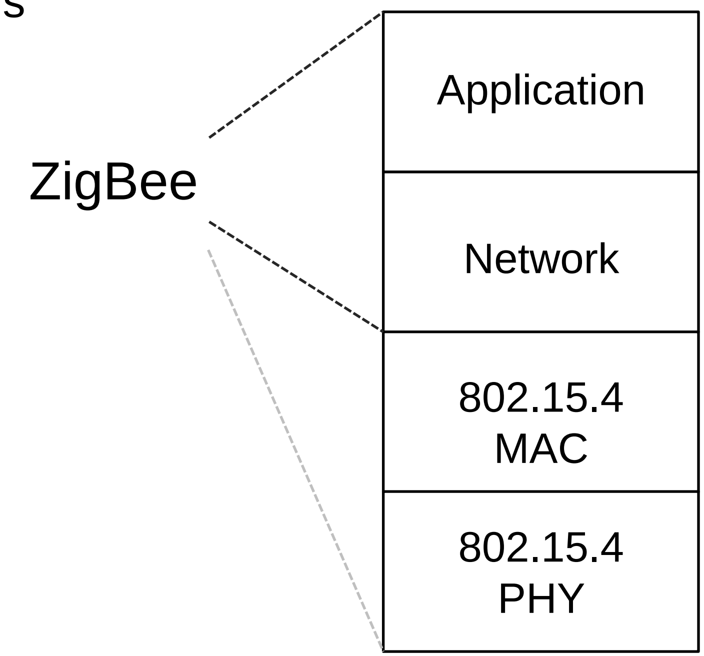




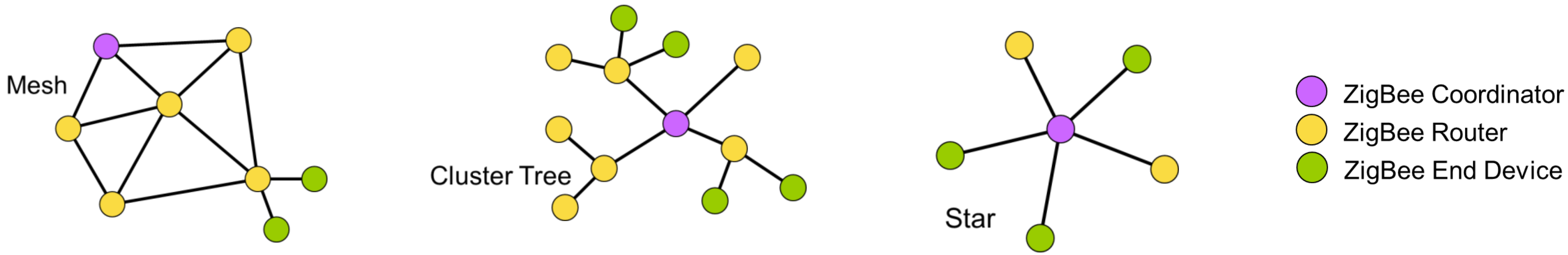
- Link Layer
- Low latency connection



- Zigbee alliance
- Based on IEEE 802.15.4
- Open Source
- ZigBee defined its own network and application layers
- Two unlicensed 802.15.4 bands in Europe
  - 868 MHz / 1 channel / 20 Kbps
  - 2,4 GHz / 16 Channels / 250 Kbps
- Range
  - ~10m
- 65,536 nodes
- Optimized for power management
  - ~Years
- Routing
  - Distance vector based
- Zigbee 3.0 I
  - supports IPv6
  - 128-b AES encryption
  - ZigBee Smart Energy Profile



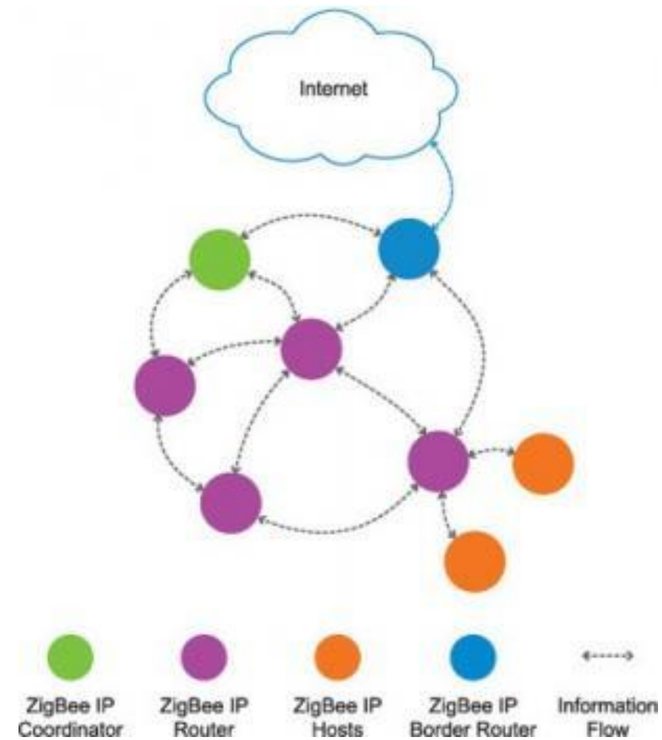
- ZigBee Coordinator (ZC)
  - One required for each ZigBee network
  - Initiates network formation
- ZigBee Router (ZR)
  - Participates in multi hop routing of messages
- ZigBee End Device (ZED)
  - Does not allow association or routing



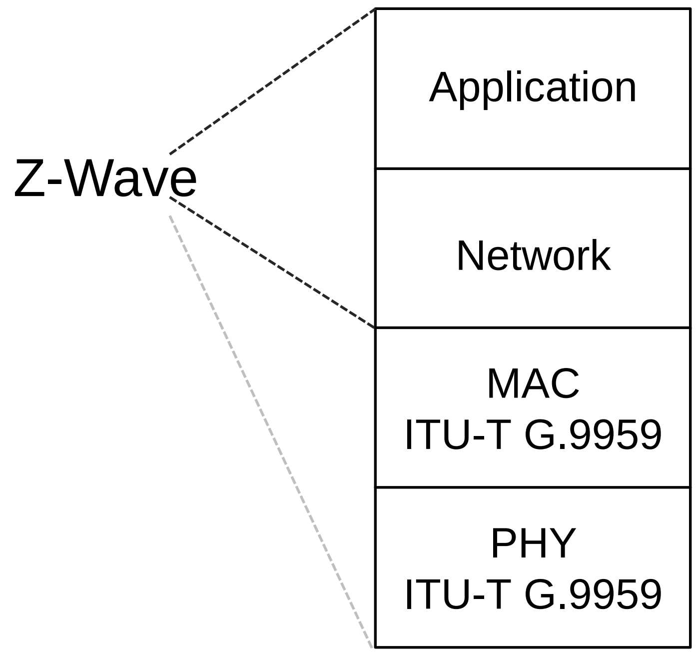
Source – ZigBee Alliance

ZigBee evolution

	ZigBee RF4CE		ZigBee PRO						ZigBee IP
Application Standard	ZigBee Remote Control	ZigBee Input Device	ZigBee Building Automation	ZigBee Health Care	ZigBee Home Automation	ZigBee Retail Services	ZigBee Smart Energy 1.x	ZigBee Telecom Services	ZigBee Smart Energy 2.0
Network	ZigBee RF4CE		ZigBee PRO						ZigBee IP
MAC	IEEE 802.15.4 – MAC								IEEE 802.15.4 - MAC
PHY	IEEE 802.15.4 Sub-GHz (specified per region)			IEEE 802.15.4 – 2.4 GHz (worldwide)					IEEE 802.15.4 2006 - 2.4GHz or other



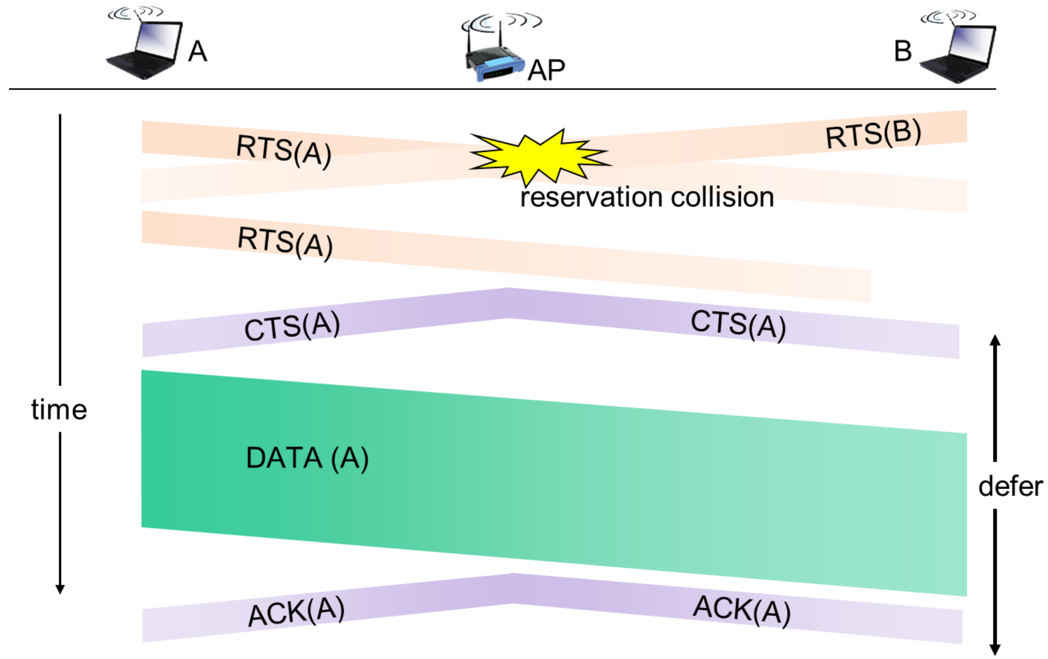
- Z-Wave
  - 1999 Zensys
- Z-Wave Alliance
- Mesh topology
- Routing
  - Nodes as hops
- node ID
  - 8-bit identifier
- 232 nodes
- 32 bits address
- CSMA/CA
- Frame size 20-30 bytes
- checksum
- ISM 868.42 MHz FSK / GFSK



Z-Wave vs ZigBee

Variable	Z-Wave	ZigBee
Year first launched in Market	2003	2003
PHY/MAC Standard	ITU-T G.9959	IEEE 802.15.4
Frequency Band	900 MHz*	2.4 GHz
Nominal Range (0 dBm)	30 – 100 m	10 – 100 m
Maximum Data Rate	40-100 kbit/s	250 kbit/s
Topology	Mesh	Mesh
Power Usage	Low	Low
Alliance	Z-Wave Alliance	ZigBee Alliance

- IEEE
- CSMA/CA
- RTS/CTS
- Architecture
  - Ad hoc
  - Infrastructure
- …



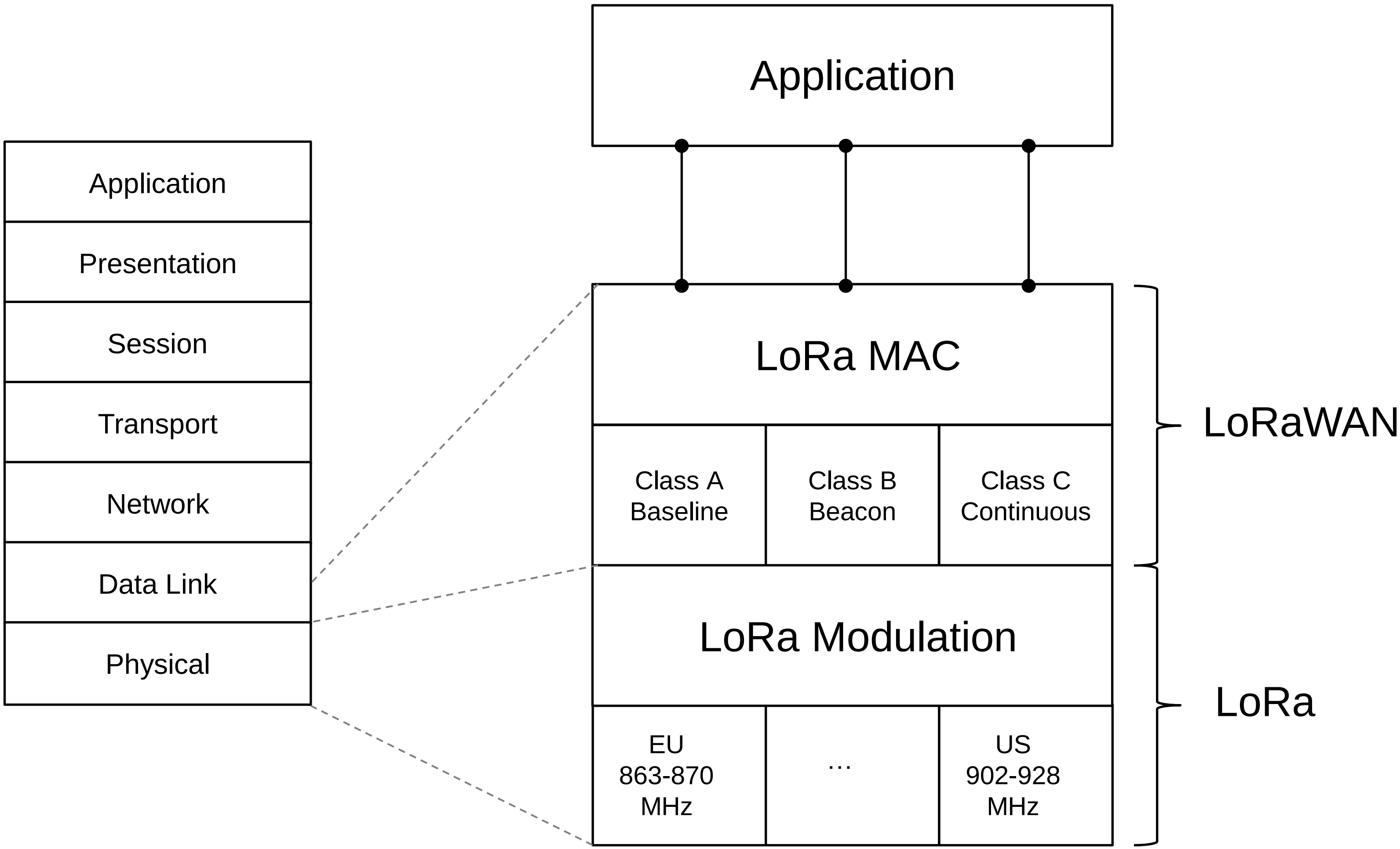
IEEE 802.11	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600 Mbps	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz
802.11ax (WiFi 6)	2020	14 Gbps	70m	2.4, 5 Ghz

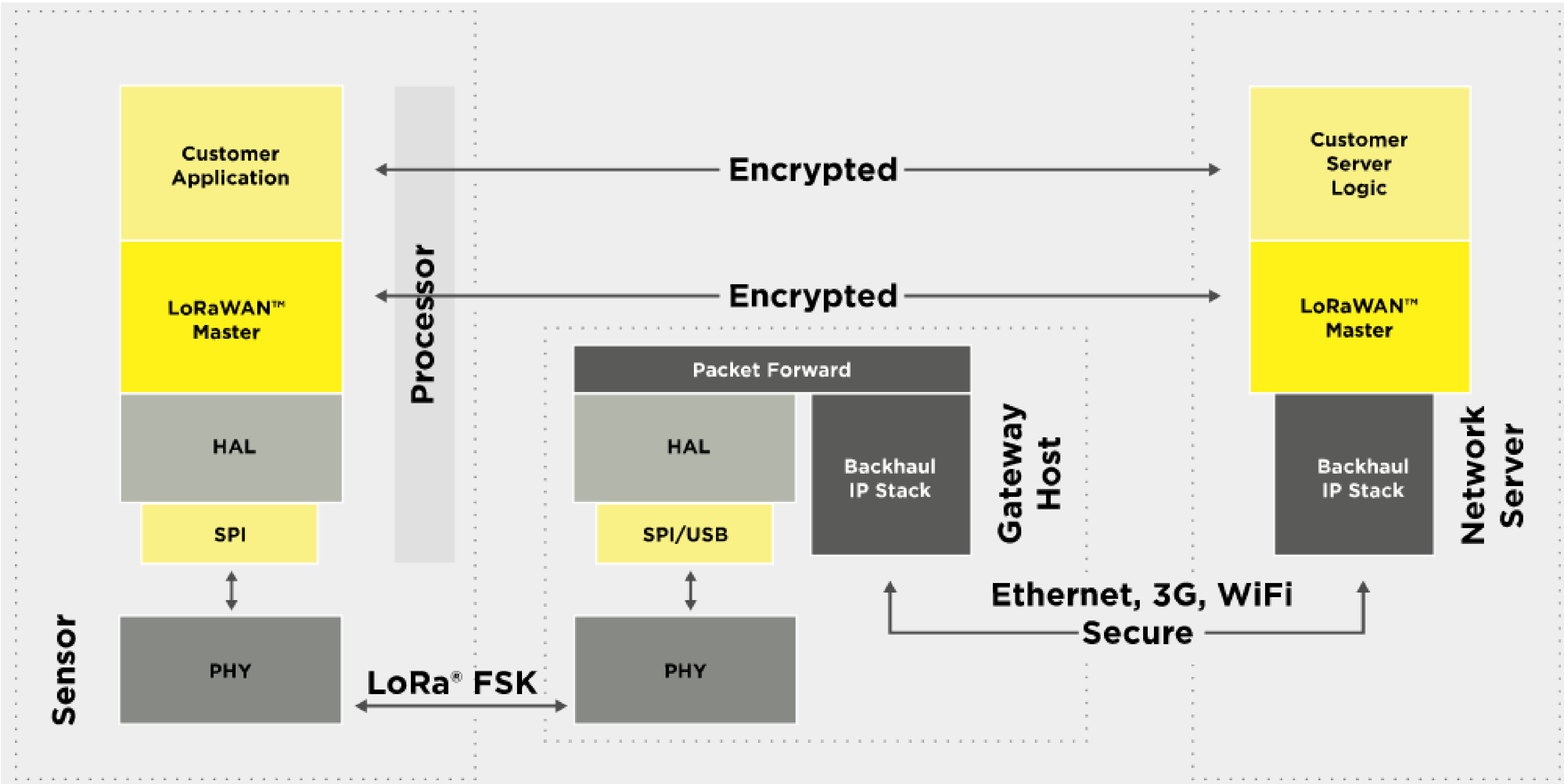
- Lightweight version of IEEE 802.11 standard to meet IoT needs.
- Original Wi-Fi standards not suitable for IoT applications
  - frame overhead
  - high power consumption.
- 802.11ah
  - low overhead,
  - power friendly communication suitable for “things” (e.g. sensors)
- 802.11ah MAC layer features include
  - Delay can be configured by the access points in 802.11ah and announced by transmitting asynchronization frame at the beginning of the transmission cycle
  - Efficient Bidirectional Packet Exchange: Allowing both uplink and downlink communication betweenaccess points and the sensors is a feature in IEEE 802.11ah.
  - Sensors will go to sleep as soon as they finish their communication
  - frame size from 30 bytes to 12bytes.
  - acknowledgment frames replaced by a
  - Such feature would add lots of overhead, especially for IoT. 802.11ah solves this problem byintroducing a tiny signal, called preamble, which is used in place of ACKs and is much less in size.-Increased Sleep Time: As this standard is designed for power constrained devices, it allows a longsleep period and waking up infrequently to exchange data only

- Work in progress
  - 802.11ax – Increased throughput in 2.4, 5 (and 6) GHz bands. Increased efficiency.
  - 802.11ay – Support for 20 Gbps in 60 GHz band.
  - 802.11az – 2nd generation positioning features.
  - 802.11ba – Wake up radio. Low power IoT applications.
  - 802.11bb – Light Communications
  - 802.11bc – Enhanced Broadcast Service
  - 802.11bd – Enhancements for Next Generation V2X
  - 802.11be – Extremely High Throughput
  - 802.11bf – WLAN Sensing [pending approval]
- 802.11az 2nd generation positioning
  - accurate location
  - Accurate indoor location
  - Secured positioning
  - Location for home usages
  - Dense environments

RFID	NFC	BLE	802.15.4	Z-Wave	802.11ah	
ISO/IEC 18000, 29167, 20248	ISO/IEC 14443, 18092	IEEE 802.15.1	IEEE 802.15.4	ITU-T G.9959	IEEE 802.11ah	
6 MHz / 865-870 MHz ISM: 2n4 GHz	13,56 MHz	2,4 GHz	868 MHz 2,4 GhHz	868 MHz	Sub-1GHz	
500 kpbs	106 kbps / 212 / 424 / 848 Kbps	1 Mbps	20 Kbps 250 Kbps	9,6, 40, 100	0,15 – 4 Mbps 0,65 è 7,8 Mbps	
0,1 – 5m	0,1 m	70 m	10 – 100 m	100 m	100 m – 1000 m	
		8 – 47 Bytes	100 Bytes	255 bits	100 bytes	

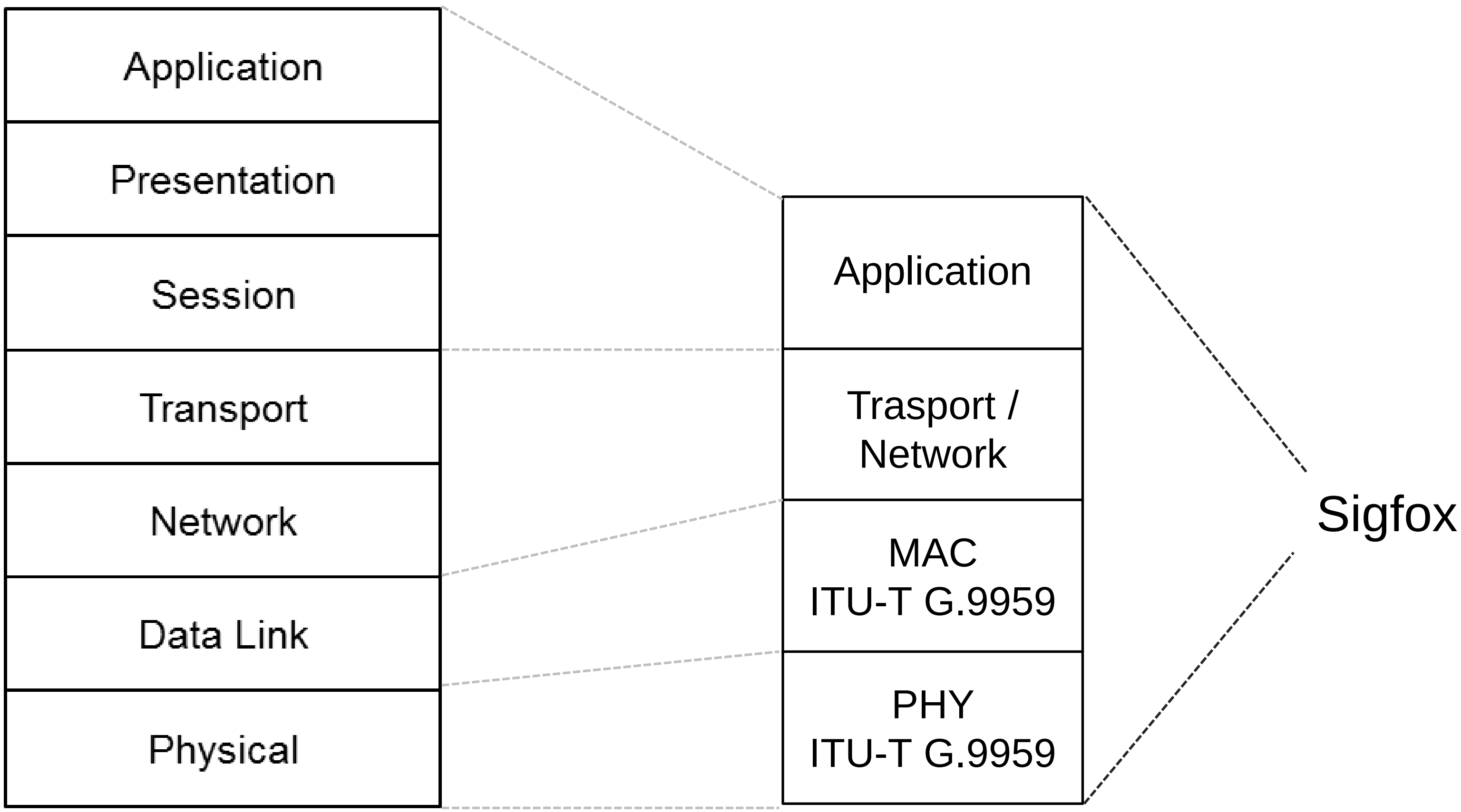
- Long Range Radio / Long Range Radio Wide Area Network
- LPWAN
- Open
- LoRa
  - Physical Layer
- LoRaWAN
  - Protocol layer
- Unlicensed frequency
  - 863-870 MHz Europe
- Modulation: a version of Chirp Spread Spectrum (CSS) with a typical channel bandwidth of 125KHz
- Range ~15 Km


Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
LoRa MAC
Class A
Baseline
Class B
Beacon
Class C
Continuous
LoRaWAN
LoRa Modulation
EU
863-870
MHz
…
US
902-928
MHz
LoRa

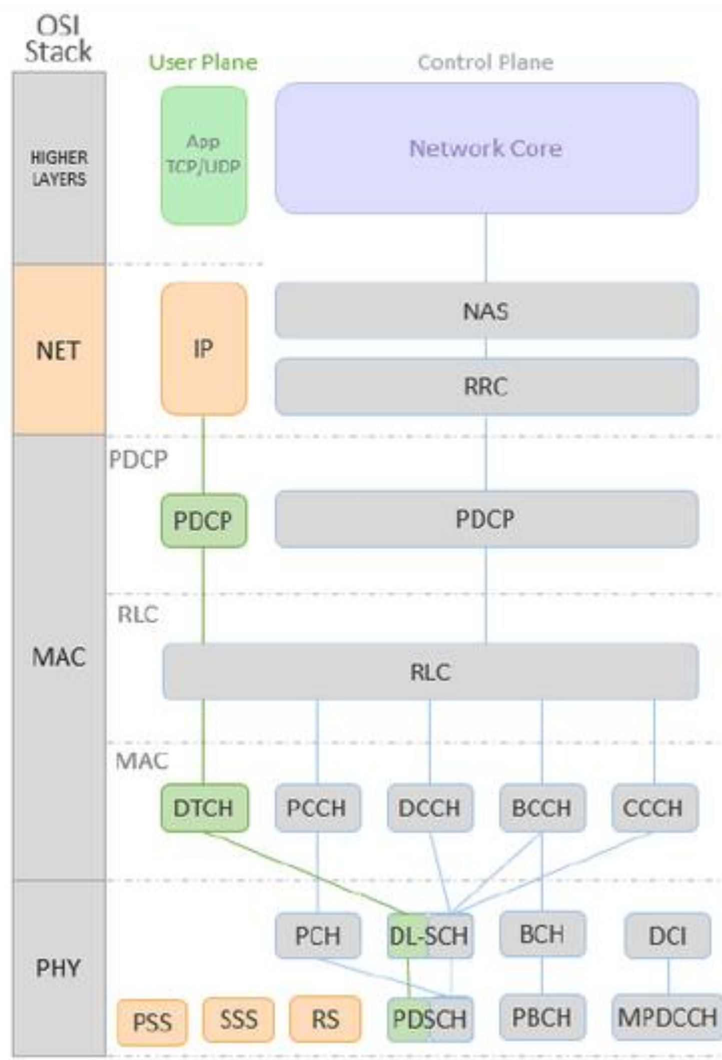


Source: LoRa Alliance

- Proprietary
- 868 MHz in Europe
- Maximum of 140 messages de 12 octets / day
- 12 bytes long on a 100 Hz channel
- Range ~3 to 50 km
- 100 bps
- Mobility restricted to 6 km/h

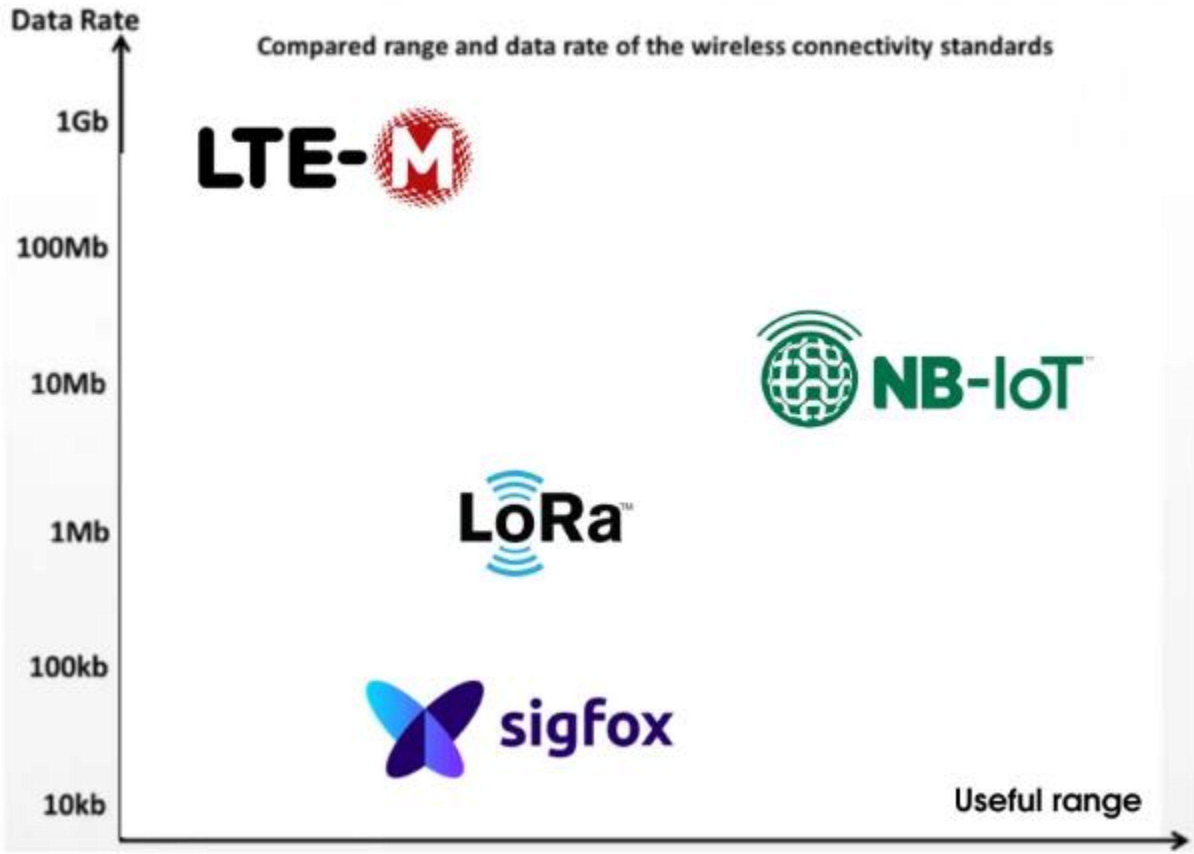

Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Trasport /
Network
MAC
ITU-T G.9959
PHY
ITU-T G.9959
Sigfox

- 3GPP standardized
- 4G LTE evolution
- LTE-MTC
  - Machine Type Communication
- IoT usage
- Licensed Spectrum
- Low power consumption and extended autonomy
- IP-Based
- Interoperability with LTE networks
- Low overall cost
- Coverage ~10 Km
- Maximum throughput ≤ 1 Mbps
- Bandwidth 700-900 MHz for LTE
- LTE-M Cat-0
  - From 3GPP release 12, LTE now supports a new UE category. LTE Category 0 or Cat 0 devices will save battery life significantly.
- Here are the biggest changes in Cat 0
- Uplink and Downlink throughput is now reduced to 1 Mbps
- UE can have now 1 antenna instead of 2
- Reduced UE receive bandwidth to 1.4 MHz allows for substantial complexity reduction
- The UE will still be able to operate in all existing LTE system bandwidths up to 20 MHz
- A lower UE power class will allow integration of power amplifier in single chip solution



- LPWAN
- 4G LTE evolution
- 3GPP standardized
- Narrow-Band IoT wireless technology
- LTE platforms add-on
- 200 Khz / OFDM 20 Kbps à 250 Kbps (download)
- NB-IoT Things
- Stakeholders : Huawei, Ericsson, Nokia, China Telecom, AT&T, Vodafone, Matooma (carte SIM LTE-M), …
- Consumption reduced (~5/10 years)

LPWAN comparison



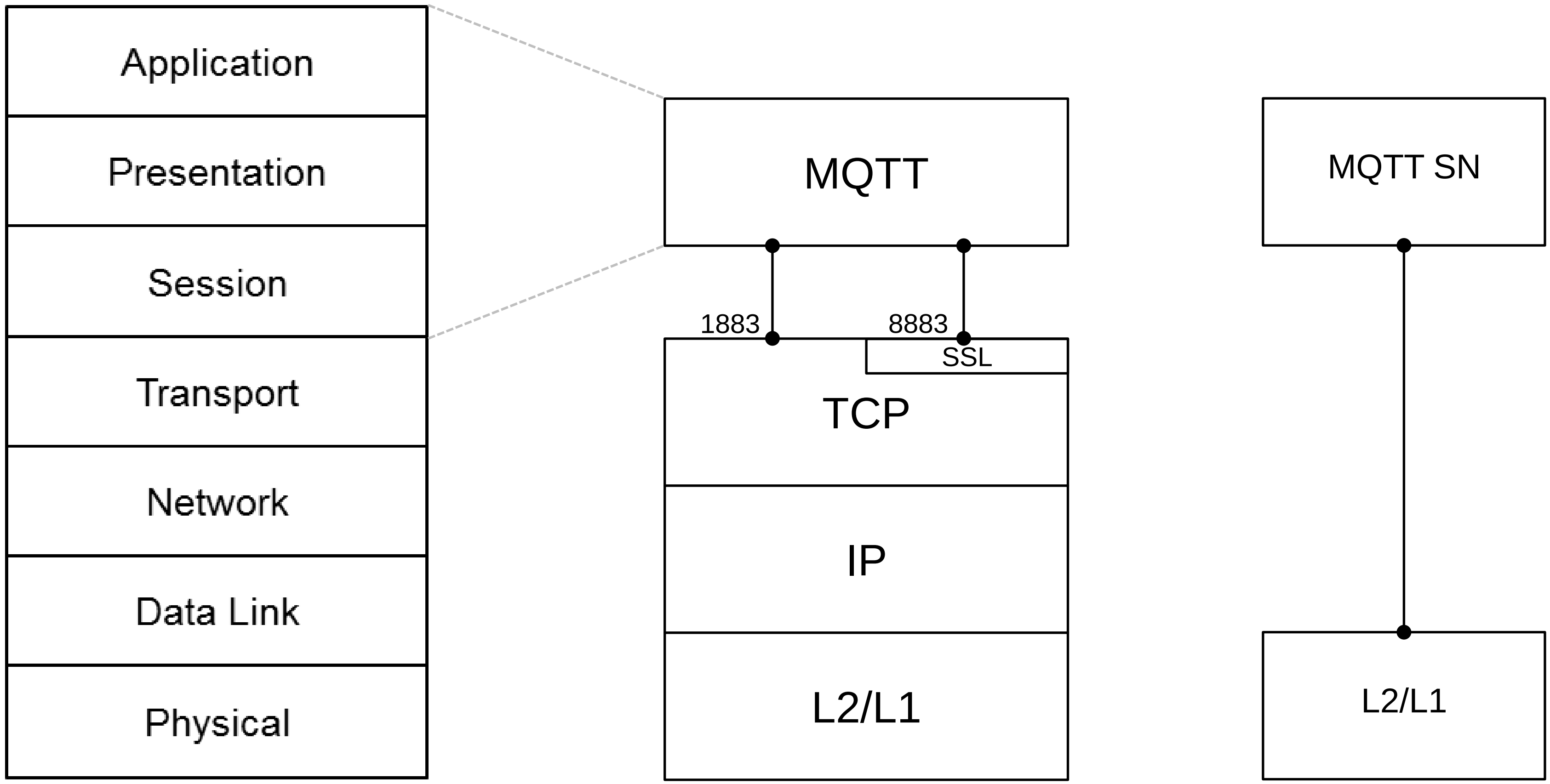
- L5/L7 competitors
  - MQTT
  - MQTT-SN
  - SNMP
  - CoAP
  - XMPP
  - AMQP
  - REST HTTP *
  - Websocket
  - LLAP
  - LWM2M
  - XMPP-IOT
  - ONS 2.0
  - SOAP
  - HTTP/2
  - …

* HTTP not suitable for IoT ?
  - https://realtimelogic.com/articles/The-scalability-problem-with-using-HTTPS-for-M2M
  - https://cloud.google.com/blog/products/iot-devices/http-vs-mqtt-a-tale-of-two-iot-protocols
  - https://www.seeedstudio.com/blog/2020/05/28/what-is-mqtt-and-why-mqtt-is-ideal-for-iot-m/

- Message Queuing Telemetry Transport
- Andy Stanford-Clark (IBM), Arlen Nipper (Arcom, now Cirrus Link) back in 1999
  - Pipeline monitpring, Scada framework
- M2M lightweight protocol
- Sensor Networks
- Embedded devices on non-TCP/IP networks
- Publish/subscribe
- ISO/IEC 20922
- Over TCP
  - 1883 MQTT
  - 8883 MQTT TLS (Secure MQTT)
  - Protocol with minimal battery loss and bandwidth connecting oil pipelines over satellite connections.
  - Simple to implement
  - Provide a QoS
  - Bandwidth Efficient
  - Data Agnostic
  - Continuous Session Awareness
- mqtt.orgsite

https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf

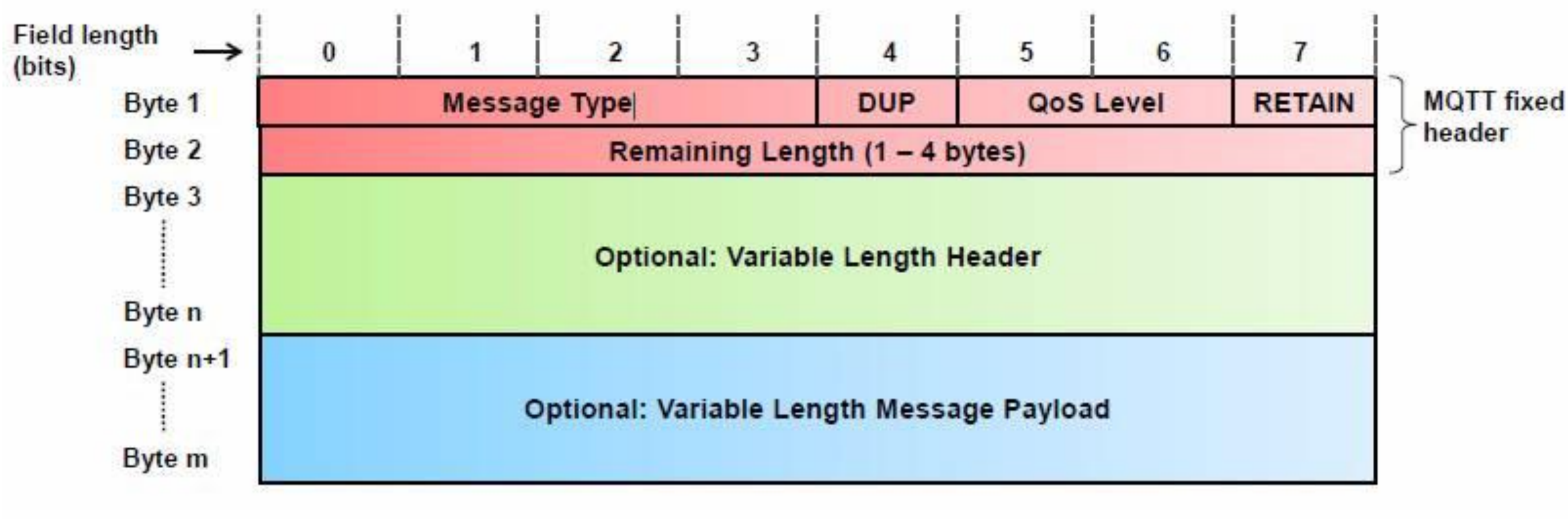
MQTT / MQTT SN


Application
Presentation
Session
Transport
Network
Data Link
Physical
MQTT
1883
8883
SSL
TCP
IP
L2/L1
MQTT SN
L2/L1

- Three parts
  - Broker
  - Subscribers
  - Publishers
- One Publisher to Many Subscribers through a Broker
- Publishers send messages over a channel (Topic)
- Subscribers read messages by monitoring Topics
- Brokers (server) act as intermediate systems between publishers and subscribers
- up to 256 Mbyte
- Asynchronous protocol
- Decoupling subscriber / publisher
- Message's type
  - Text
  - Images
  - etc.
- Message
  - topic,
  - quality of service,
  - retain status

MQTT: message structure

- Shortest Message is Two Bytes



MQTT: message type

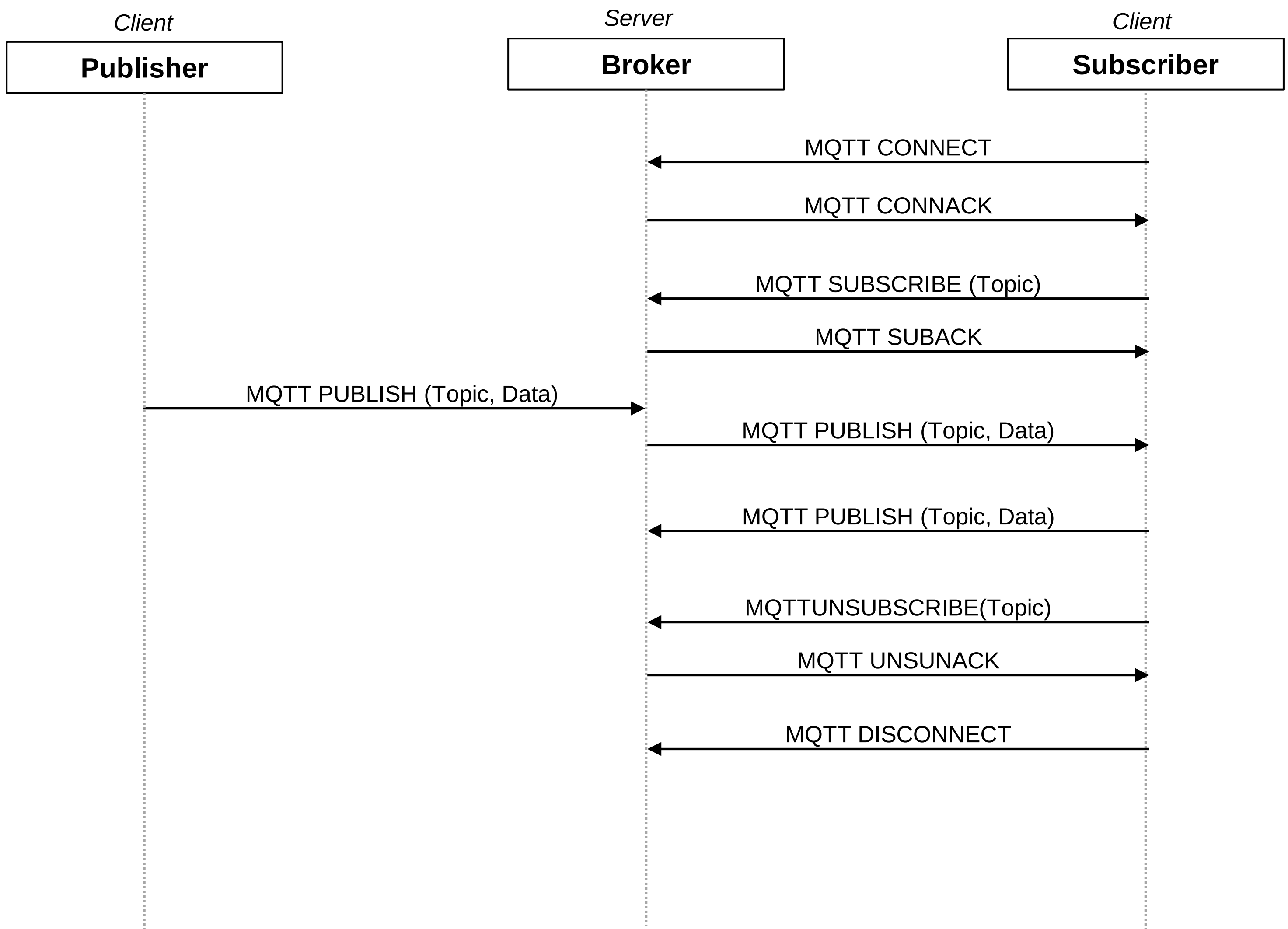
Message fixed header field	Description / Values	
Message Type	0: Reserved	8: SUBSCRIBE
	1: CONNECT	9: SUBACK
	2: CONNACK	10: UNSUBSCRIBE
	3: PUBLISH	11: UNSUBACK
	4: PUBACK	12: PINGREQ
	5: PUBREC	13: PINGRESP
	6: PUBREL	14: DISCONNECT
	7: PUBCOMP	15: Reserved
DUP	Duplicate message flag. Indicates to the receiver that this message may have already been received. 1: Client or server (broker) re-delivers a PUBLISH, PUBREL, SUBSCRIBE or UNSUBSCRIBE message (duplicate message).	
QoS Level	Indicates the level of delivery assurance of a PUBLISH message. 0: At-most-once delivery, no guarantees, «Fire and Forget». 1: At-least-once delivery, acknowledged delivery. 2: Exactly-once delivery. Further details see MQTT QoS.	
RETAIN	1: Instructs the server to retain the last received PUBLISH message and deliver it as a first message to new subscriptions. Further details see RETAIN (keep last message).	
Remaining Length	Indicates the number of remaining bytes in the message, i.e. the length of the (optional) variable length header and (optional) payload. Further details see Remaining length (RL).	

MQTT: messages types

Name	Value	Direction of flow	Description
Reserved	0	Forbidden	Reserved
CONNECT	1	Client to Server	Client request to connect to Server
CONNACK	2	Server to Client	Connect acknowledgment
PUBLISH	3	Client to Server or Server to Client	Publish message
PUBACK	4	Client to Server or Server to Client	Publish acknowledgment
PUBREC	5	Client to Server or Server to Client	Publish received (assured delivery part 1)
PUBREL	6	Client to Server or Server to Client	Publish release (assured delivery part 2)
PUBCOMP	7	Client to Server or Server to Client	Publish complete (assured delivery part 3)
SUBSCRIBE	8	Client to Server	Client subscribe request
SUBACK	9	Server to Client	Subscribe acknowledgment
UNSUBSCRIBE	10	Client to Server	Unsubscribe request
UNSUBACK	11	Server to Client	Unsubscribe acknowledgment
PINGREQ	12	Client to Server	PING request
PINGRESP	13	Server to Client	PING response
DISCONNECT	14	Client to Server	Client is disconnecting
Reserved	15	Forbidden	Reserved

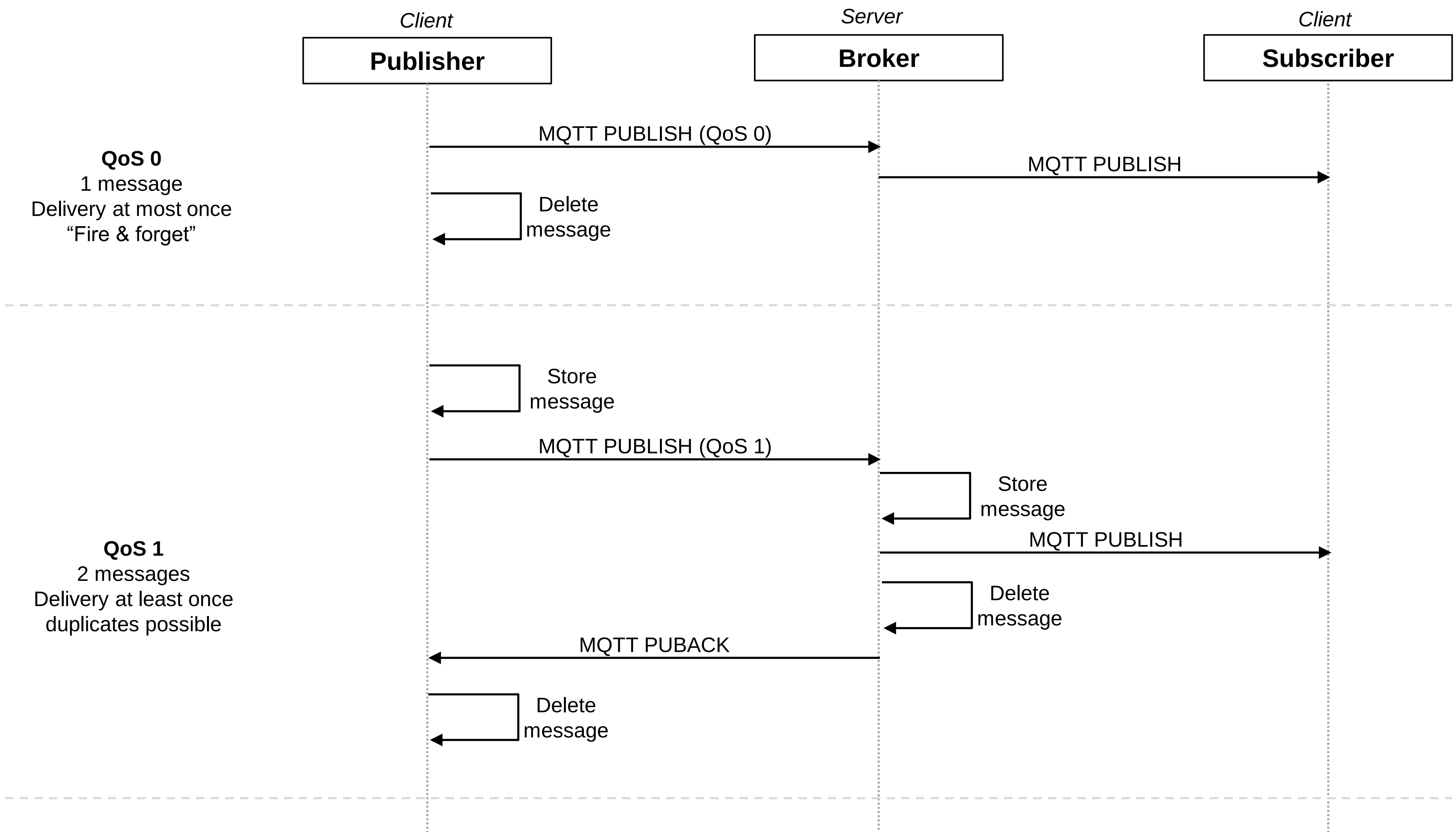
Source: morphuslabs.com

MQTT publish / subscribe principle



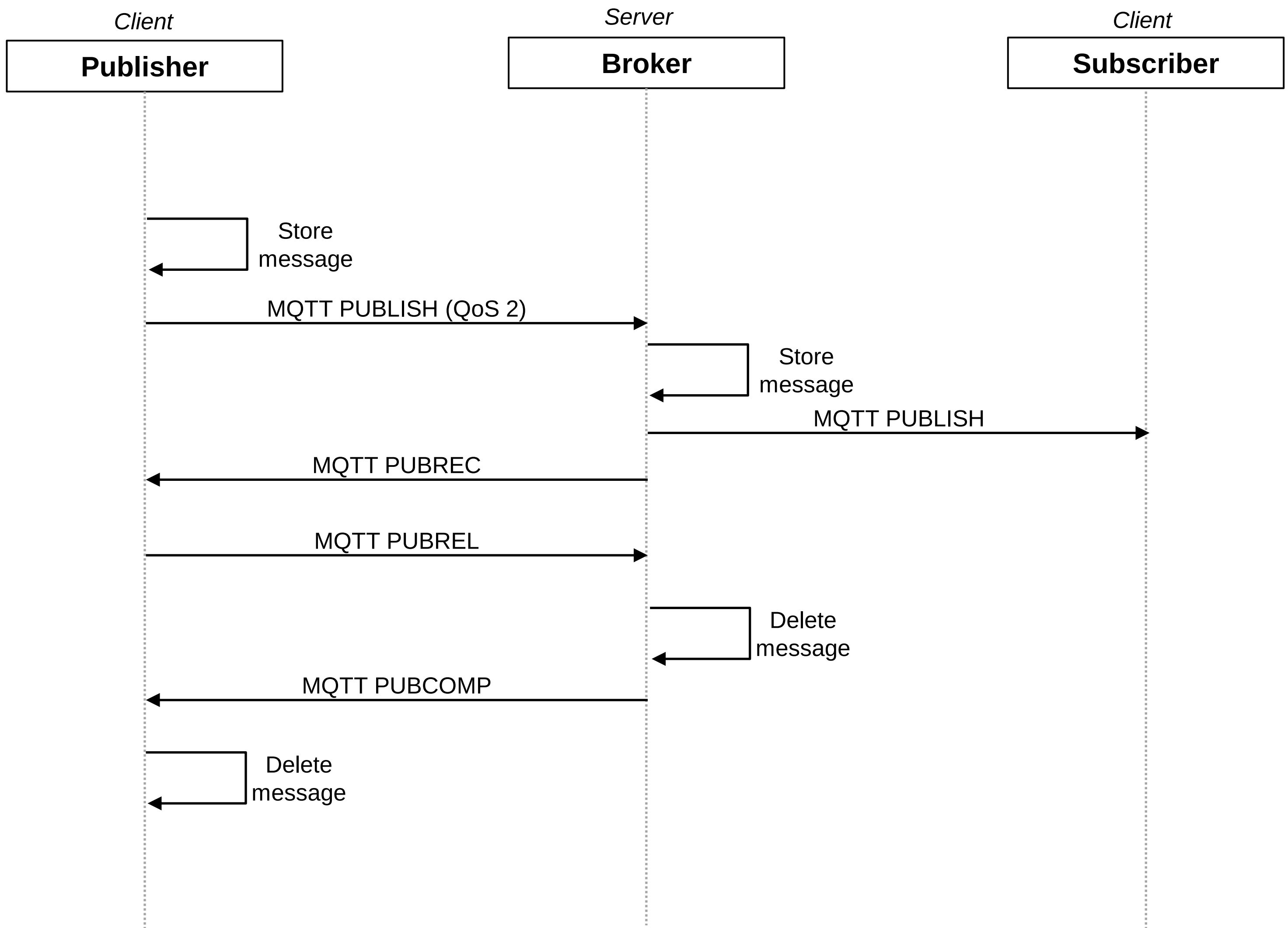
Source: MQTT.org

MQTT QoS


Client
Publisher
Server
Broker
Client
Subscriber
MQTT PUBLISH (QoS 0)
MQTT PUBLISH
QoS 0
1 message
Delivery at most once
“Fire & forget”
Delete message
Store message
MQTT PUBLISH (QoS 1)
Store message
MQTT PUBLISH
QoS 1
2 messages
Delivery at least once
duplicates possible
Delete message
MQTT PUBACK
Delete message

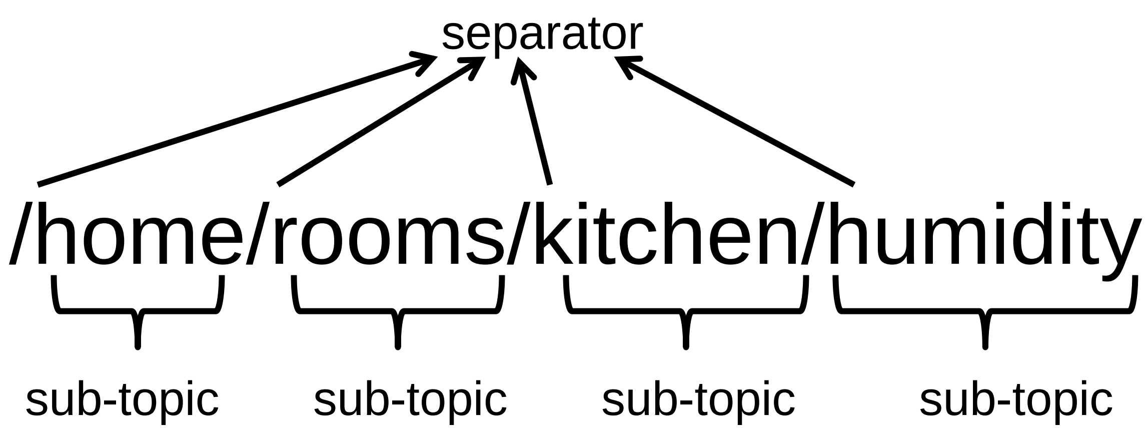
MQTT QoS

QoS 2
4 messages
Delivery exactly once



MQTT: Topics

- Each published data specifies a topic
- Each subscriber subscribed to that topic will receive it
- Topic format

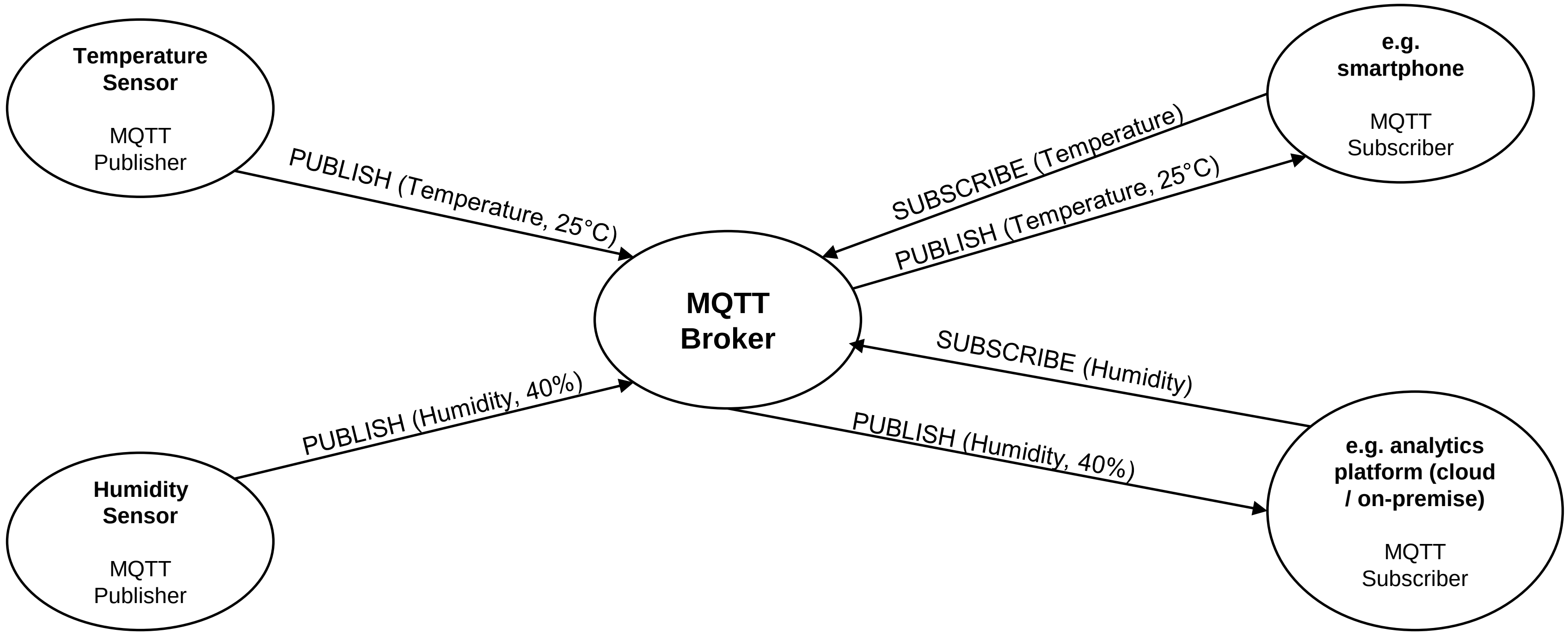


- Eclipse Mosquitto
  - open-source message broker that implements the MQTT protocol.

MQTT: example

- Clients connect to a “Broker”
- Clients subscribe to topics e.g.,
  - client.subscribe(‘toggleLight/1’)
  - client.subscribe(‘toggleLight/2’)
  - client.subscribe(‘toggleLight/3’)
- Clients can publish messages to topics:
  - client.publish(‘toggleLight/1’, ‘toggle’);
  - client.publish(‘toggleLight/2’, ‘toggle’);
- All clients receive all messages published to topics they subscribe to
- Messages can be anything
  - Text
  - Images
  - etc.

MQTT: example



Topic #1: Humidity
Topic #2: Temperature

MQTT: Node.js example

```
var mqtt = require('mqtt');
var client = mqtt.createClient('<<PortNumber>>', 'm11.cloudmqtt.com', {
		username: '<<UserName>>’,
		password: '<<Password>>'
});
client.on('connect', function () { // When connected
		// subscribe to a topic
		client.subscribe('TEMPERATURE_READING', function () {
				// when a message arrives, do something with it
				client.on('message', function (topic, message, packet) {
						console.log("Received '" + message + "' on '" + topic + "'");
				});
		});
		// publish a message to a topic
		client.publish('SET_TEMPERATURE', '24', function () {
				console.log("Message is published");
		});
});
```

CoAP

- Constrained Application Protocol
  - REST-based web transfer protocol
  - manipulates Web resources using the same methods as HTTP: GET, PUT, POST, and DELETE
  - subset of HTTP functionality re-designed for low power embedded devices such as sensors (for IoT and M2M)
- RFC 7252
- UDP port 5683
- Client/server
- Reliability without using TCP
- Enables asynchronous communication
  - e.g., when CoAP server receives a request which it cannot handle immediately, it first ACKs the reception of the message and sends back the response in an off-line fashion
- Multicast and congestion control
- A RESTful protocol
  - Both synchronous and asynchronous
  - For constrained devices and networks
  - Specialized for M2M applications
  - Easy to proxy to/from HTTP
- Four message types
  - Confirmable – requires an ACK
  - Non-confirmable – no ACK needed
  - Acknowledgement – ACKs a Confirmable
  - Reset - indicates a Confirmable message has been received but context is missing for processing
- RFC 8323 CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets
- LWM2M

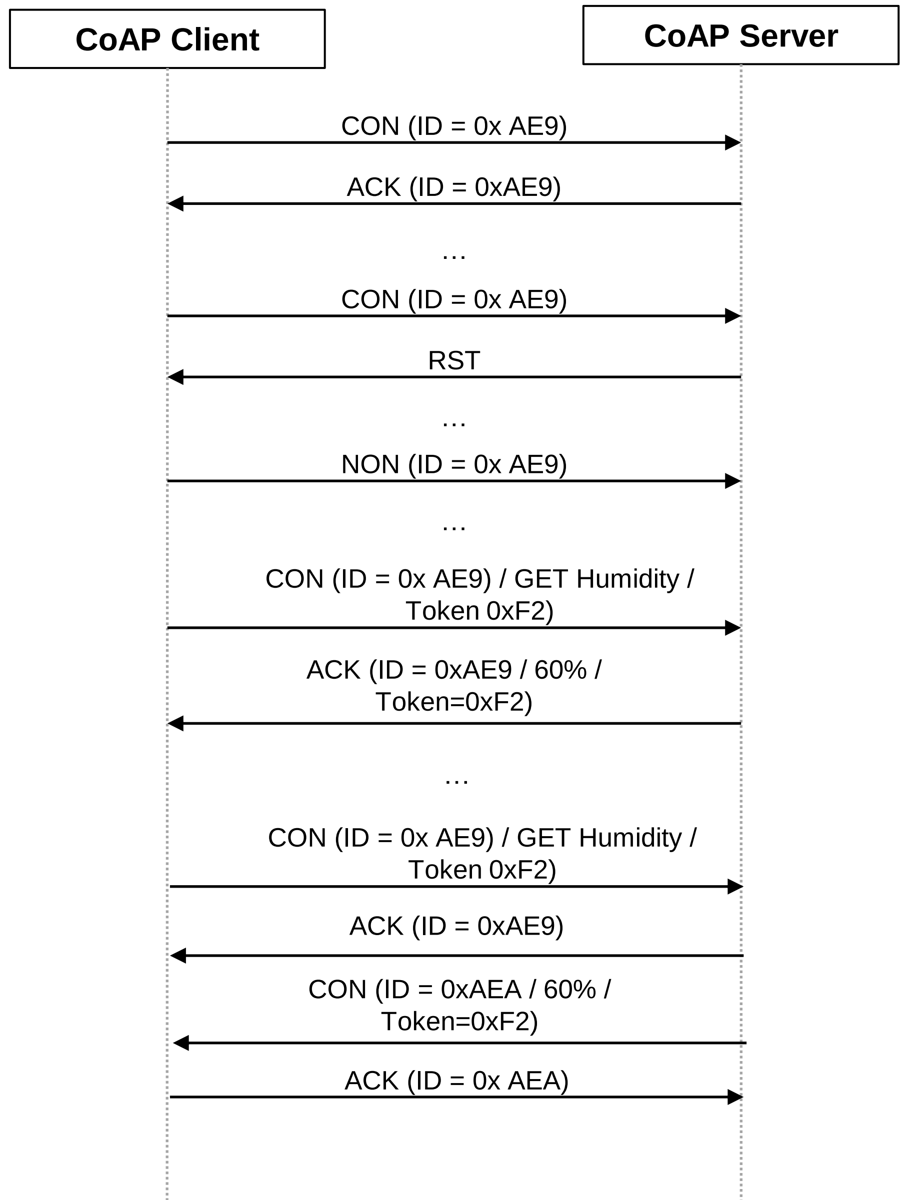
CoAP
UDP
IPv6
LoWPAN
IEEE 802.15.4

CoAP

- Version (2 Bits)
  - 1
- Message Type (2 bits)
  - 00 Confirmable
  - 01 Non Confirmable
  - 10 Ack
  - 11 Reset
- Token Length (4 bits)
- Code (4 bits)
  - 0001 GET
  - 0010 POST
  - 0011 PUT
  - 0100 DELETE
- Message ID (16 bits)
  - Message identifier
- Token (0 to 8 bytes)
  - Response Token must be resquest token
  - Token value defined by app.
- Payload
  - Payload Marker = 0xff
  - Optional
  - Format specified by Content-Format option
  - Formats: Text, JSON, XML, Binary, …

<table>
<tr><td>V</td><td>T</td><td>TKL</td><td>Code</td><td>Message ID</td></tr>
<tr><td colspan="5">Token (if any, TKL bytes) …</td></tr>
<tr><td colspan="5">Options (if any) …</td></tr>
<tr><td colspan="3">1 1 1 1 1 1 1 1</td><td colspan="2">Payload (if any) …</td></tr>
</table>

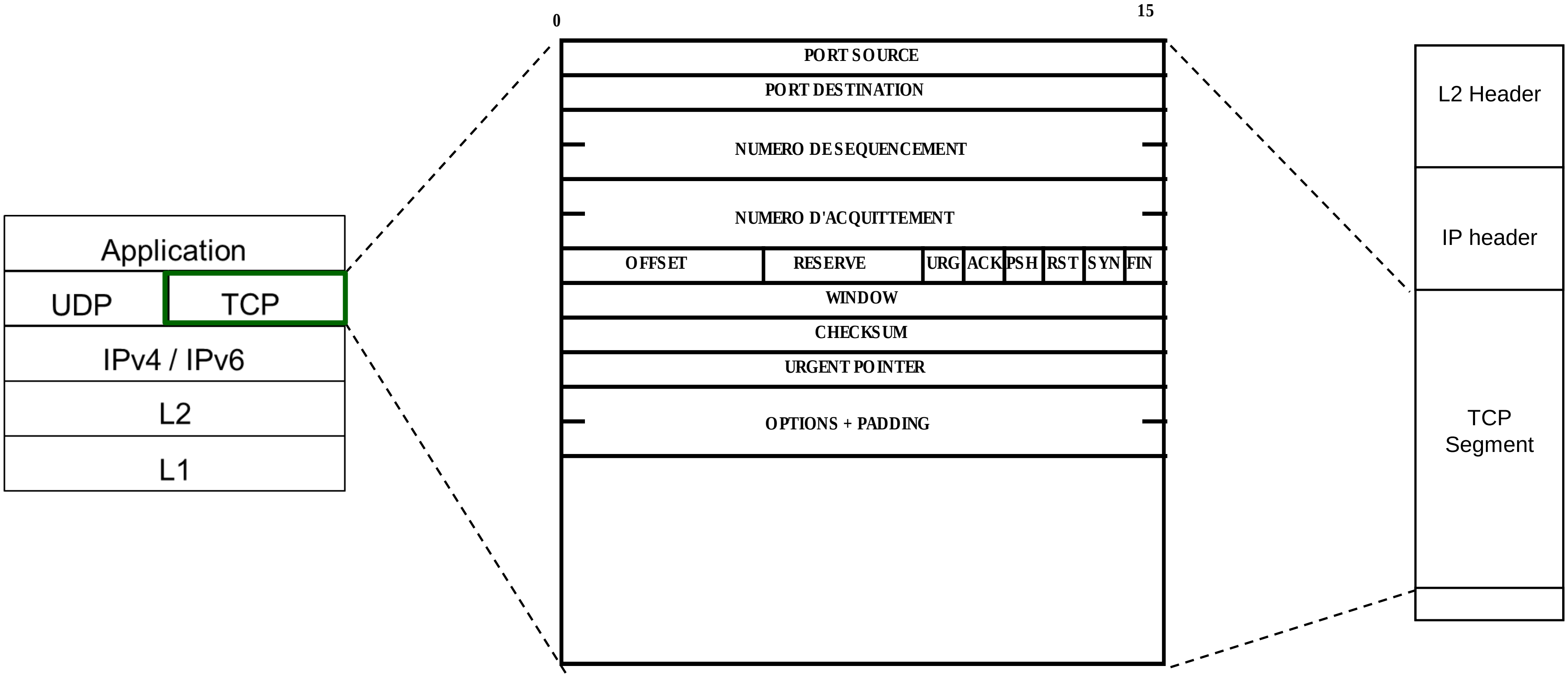
CoAP messages



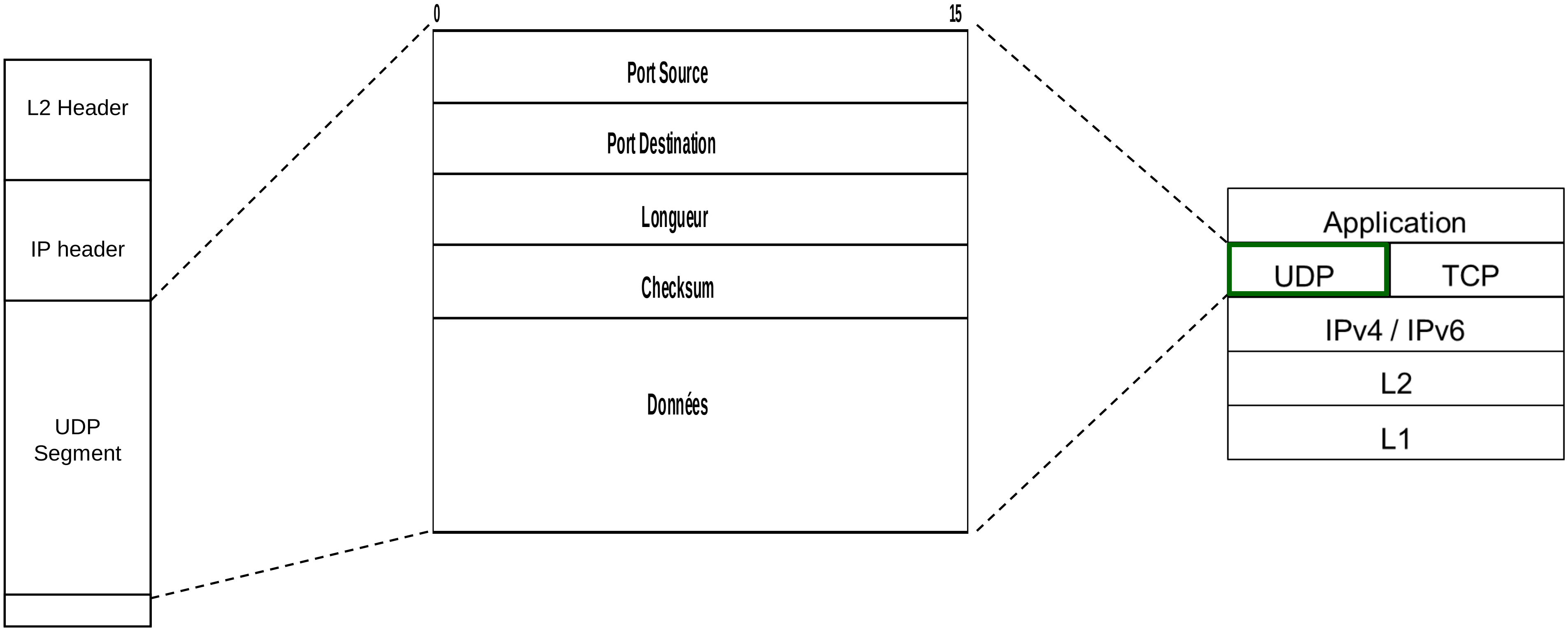
CoAP vs MQTT

	MQTT	CoAP
Communication	Publish / Subscribe	Request/Reply (REST)
Transport Layer	TCP	UDP
	TLS (not	DTLS, IPSec
Nbr of messages	16	4
Asynch. / Synch.	Asynch.	Asynch., Synch.
Header (Bytes)	2	4
…	…	…

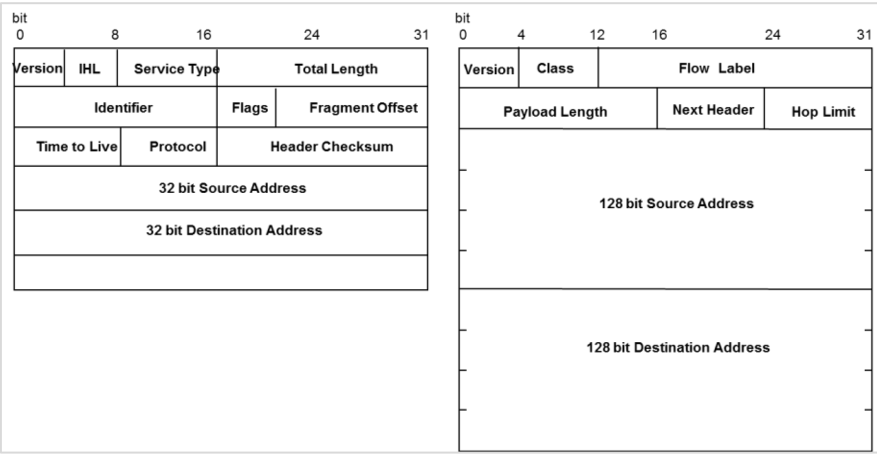
IoT: L4 protocols

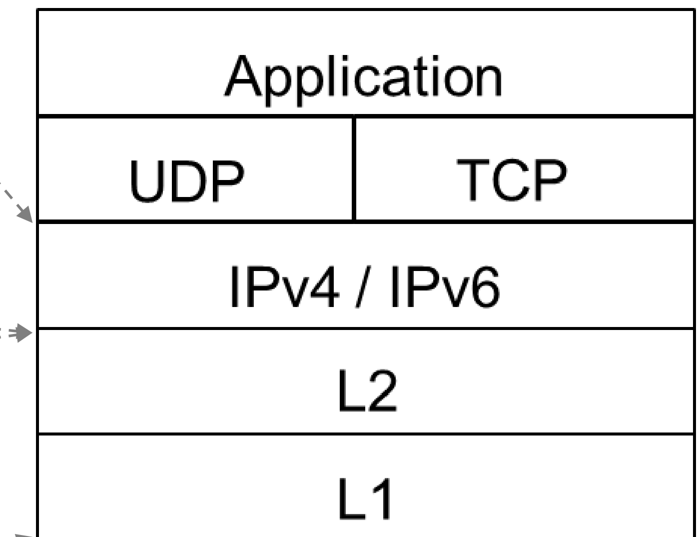


IoT: L4 protocols



IP: keystone of the IoT communication flows

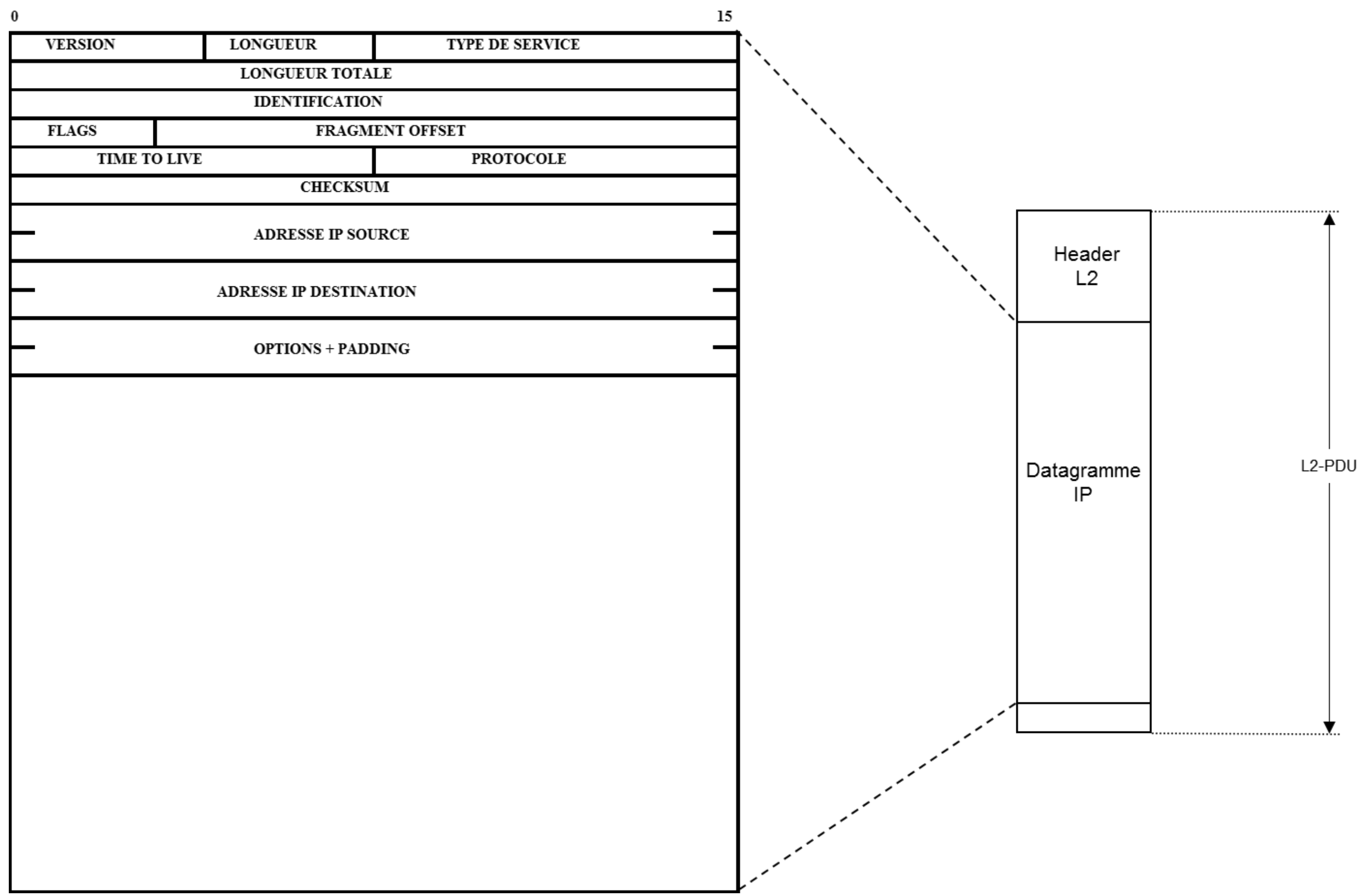




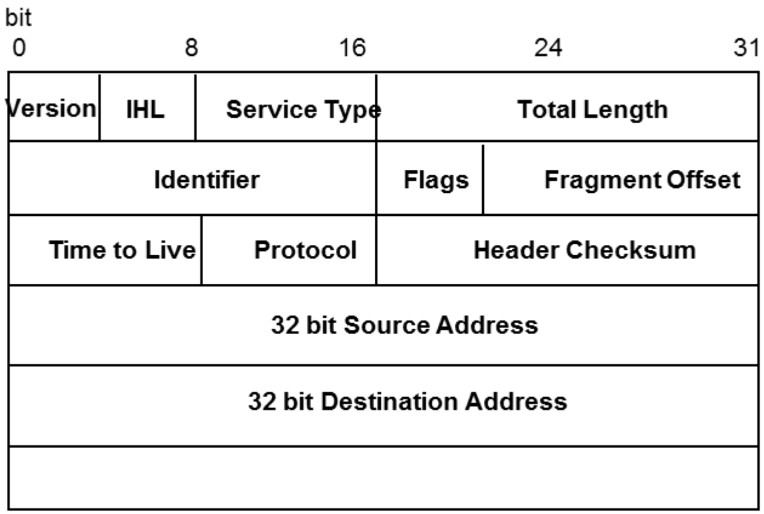
RFID / NFC
802.15.4 (ZigBee, …)
BLE
ITU-T G.9959 (Z-Wave, SigFox, …)
ZigBee
IEEE 802.11
LoRA MAC/PHY
LTE-M (eMTC)
NB-IoT

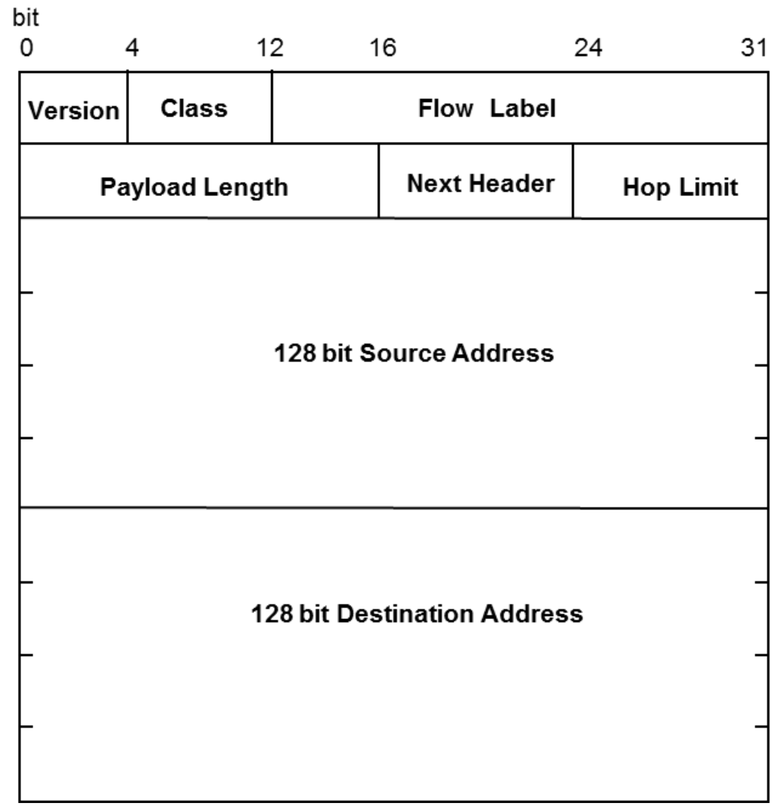
6LoWPAN: IPv4 reminder

- RFC 791
- L3
- Datagram oriented
- 32 Bits Addresses
- Fragmentation/ Reassembly
- …

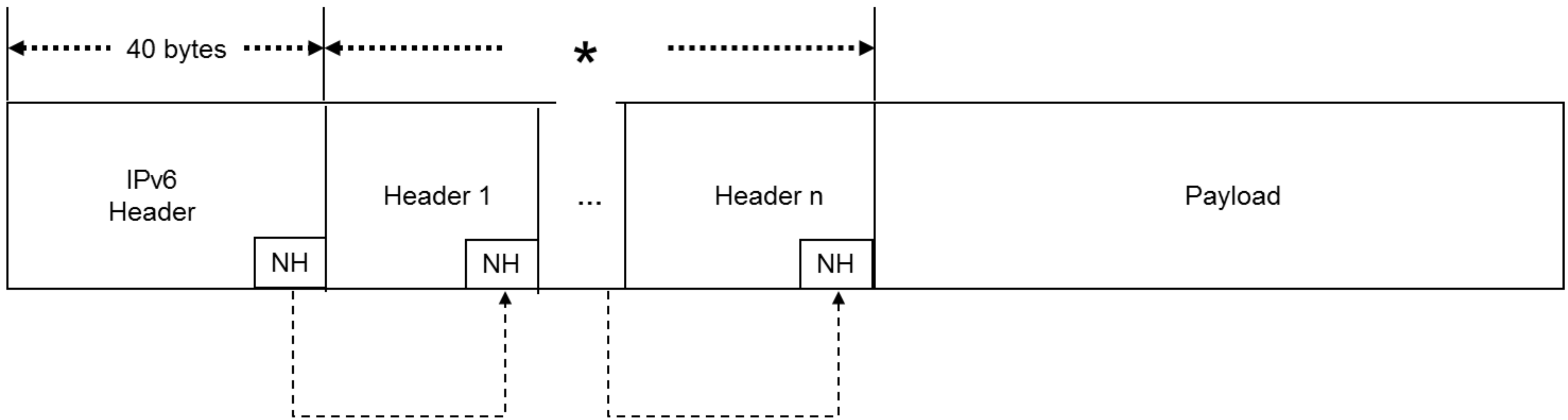


- IETF
- 1995/1996
- Lack of @ipv4 public addresses





- IPv6 extension headers
- Extension header format

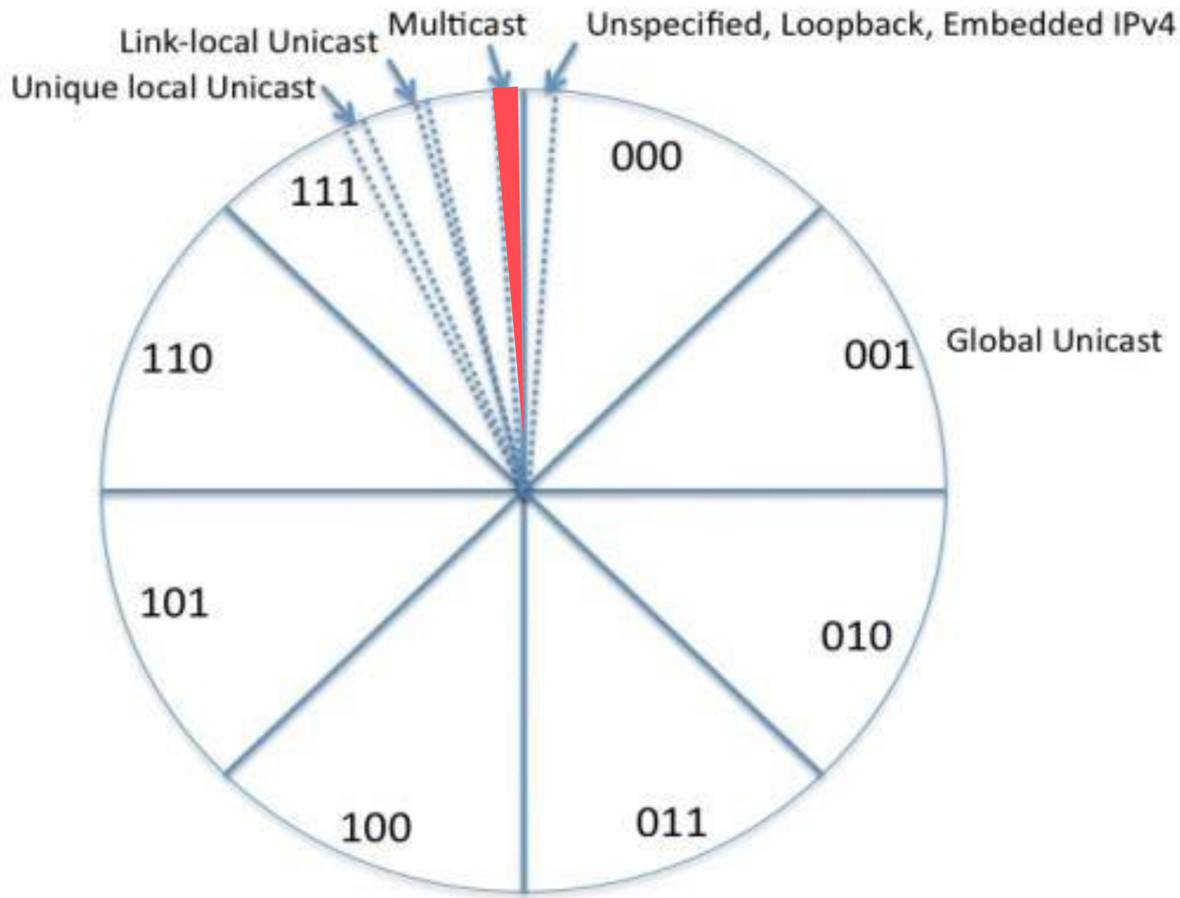


- Classless addressing
- Unicast, multicast, anycast
- Multiple addresses per interface
- Standard representation is set of eight 16-bit values separated by colons
  - Eg. 47CD:1234:3200:0000:0000:4325:B792:0428
- If there are large number of zeros, they can be omitted with series of colons
  - Eg. 47CD:1234:3200::4325:B792:0428
- Address prefixes (slash notation) are the same as v4
  - Eg. FEDC:BA98:7600::/40 describes a 40 bit prefix
- Addresses have scope
  - Link
  - Unique
  - Global

- Loopback Address
  - ::1
- Link-Local Address
  - fe80::/10
- Unique Local Address
  - fc00::/7
- Site-Local Address
  - deprecated by IETF (RFC 3879)
- Global Unicast Address
  - 2000::/3
- An interface may/will have multiple IPv6 addresses

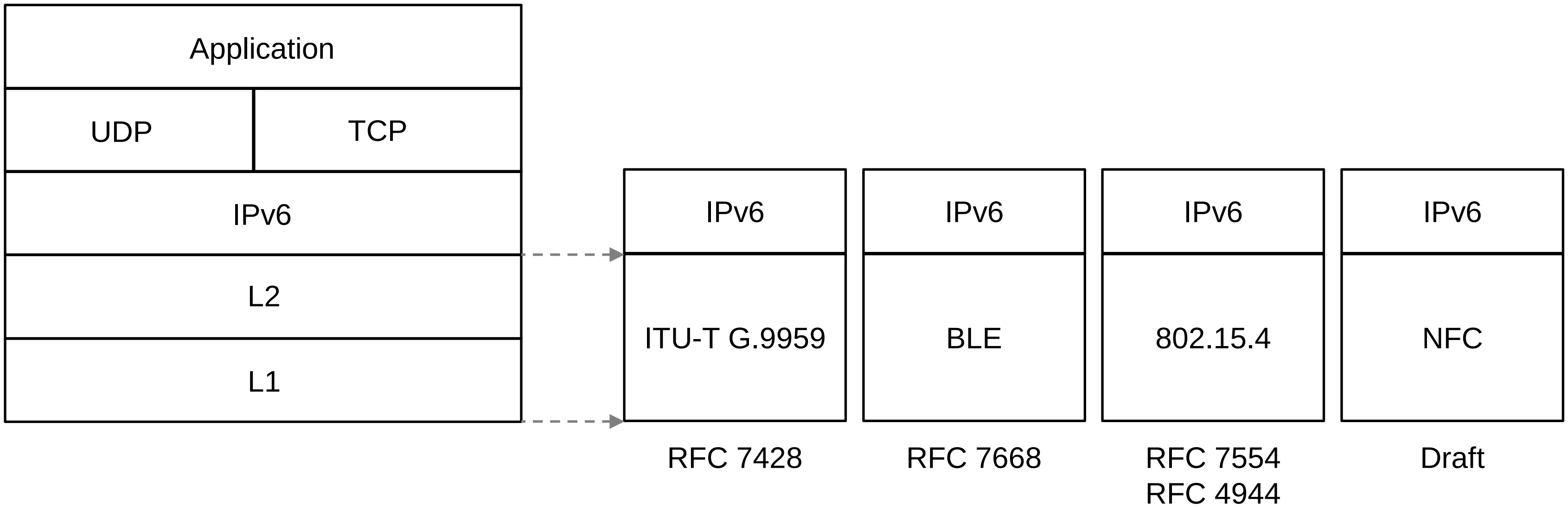
- IPv6 multicast address
- ff00::/8
- Always used as a destination address
- Scope
  - 0000 Reserved
  - 0001 Interface-Local scope
  - 0010 Link-Local scope
  - 0011 Site-Local scope
  - 1000 Organization-Local scope
  - 1110 Global scope

8 bits	4 bits	4 bits	112 bits
1111 1111	Flags	Scope	Group ID



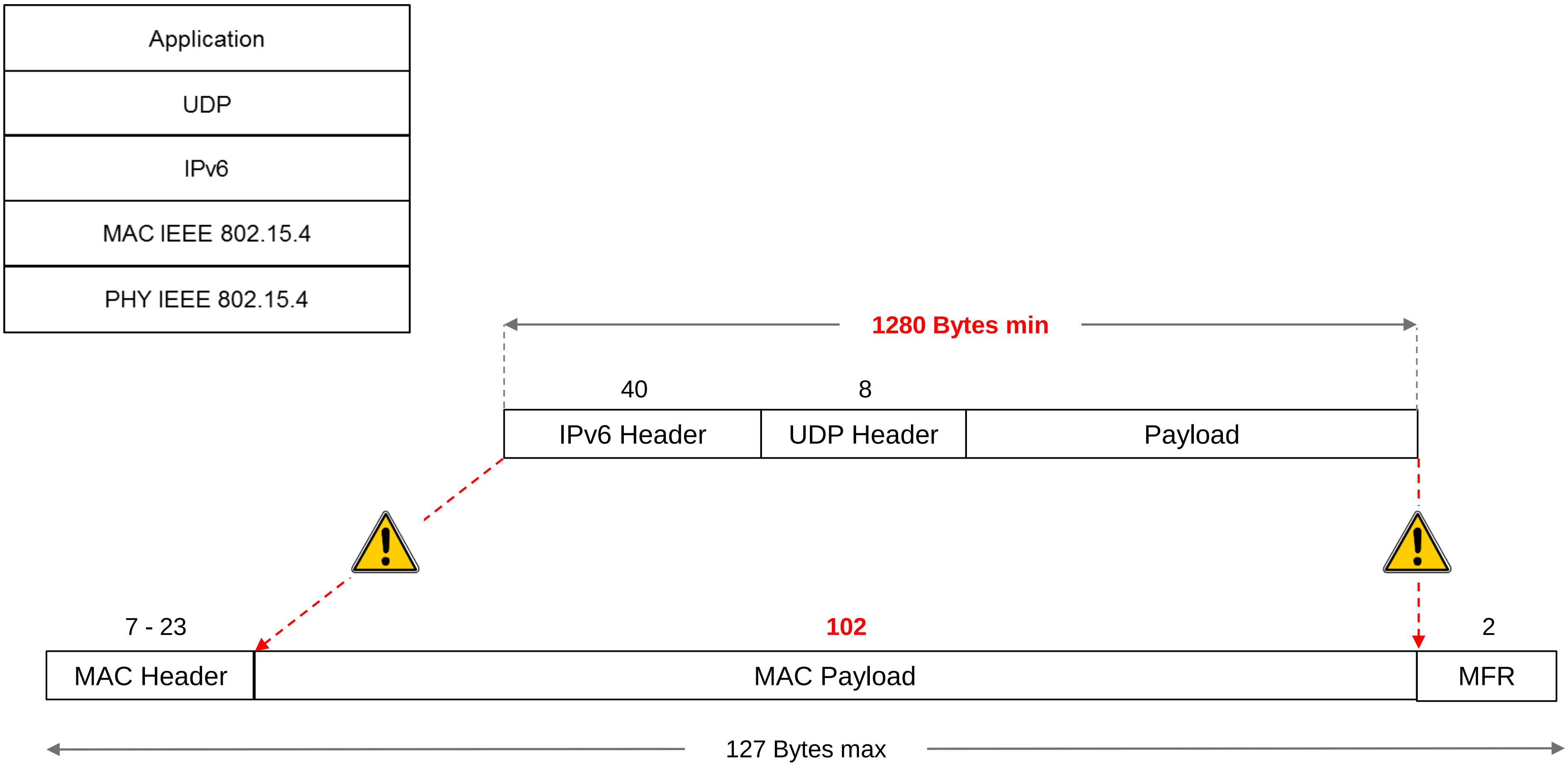
The remaining portion of IPv6 address space are reserved by IETF for future use.

6LoWPAN: IPv6 challenges over IoT L2/L1 layers

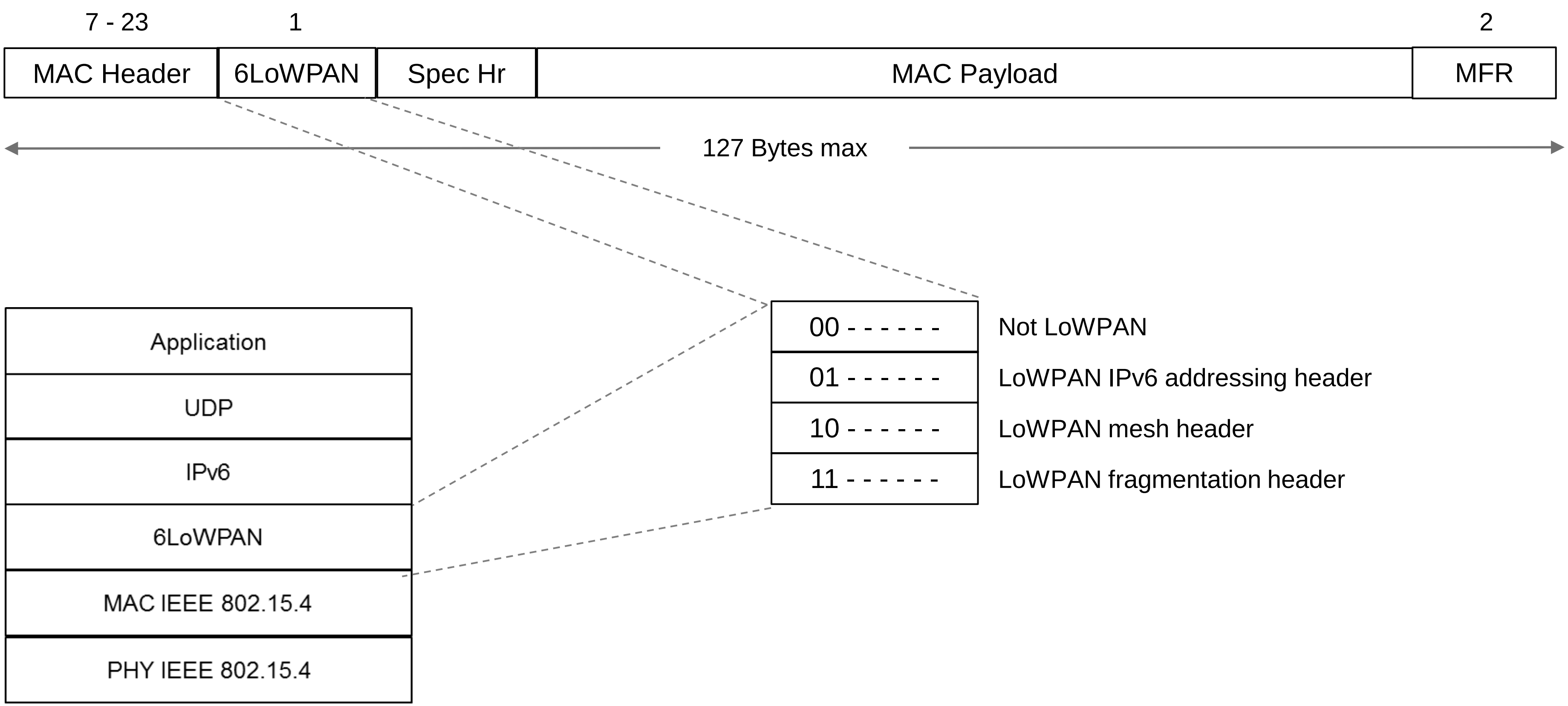


- Main issues
  - Addressing
  - MTU
  - Routing
  - Header compression
  - Security / encryption
  - …

6LoWPAN: IPv6 over 802.15.4 challenge

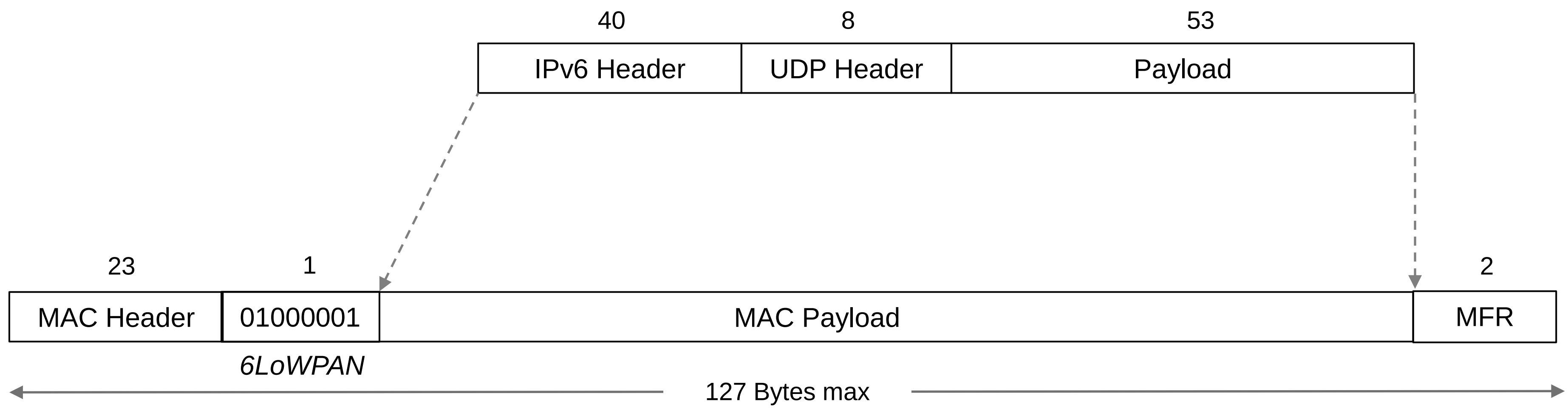


6LoWPAN: adaptation layer

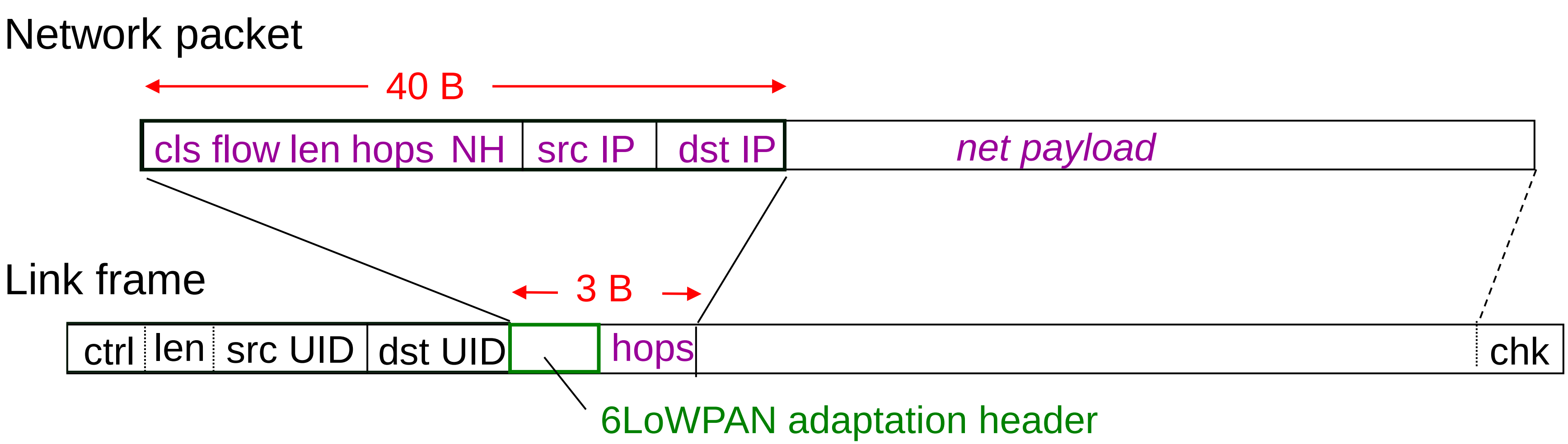


```
A LoWPAN encapsulated IPv6 datagram:
+---------------+-------------+---------+
| IPv6 Dispatch | IPv6 Header | Payload |
+---------------+-------------+---------+

A LoWPAN encapsulated LOWPAN_HC1 compressed IPv6 datagram:
+--------------+-------------+---------+
| HC1 Dispatch | HC1 Header  | Payload |
+--------------+-------------+---------+

A LoWPAN encapsulated LOWPAN_HC1 compressed IPv6 datagram that requires mesh
addressing:
+-----------+-------------+--------------+-------------+---------+
| Mesh Type | Mesh Header | HC1 Dispatch | HC1 Header  | Payload |
+-----------+-------------+--------------+-------------+---------+

A LoWPAN encapsulated LOWPAN_HC1 compressed IPv6 datagram that requires
fragmentation:
+-----------+-------------+--------------+-------------+---------+
| Frag Type | Frag Header | HC1 Dispatch | HC1 Header  | Payload |
+-----------+-------------+--------------+-------------+---------+
```

6LoWPAN over 802.15.4: uncompressed header format



- Eliminate all fields in the IPv6 header that can be derived from the 802.15.4 header in the common case
  - Source address : derived from link address
  - Destination address : derived from link address
  - Length : derived from link frame length
  - Traffic Class & Flow Label : zero
  - Next header : UDP, TCP, or ICMP



6LoWPAN over 802.15.4: challenge

- Assume common values for header fields and define compact forms
  - Version is always 6
  - Traffic Class and Flow Label are zero
  - Payload Length always derived from L2 header
  - Next Header is UDP, TCP, or ICMPv6
  - Source and Destination Addrs are link-local and derived from L2 addrs
- Eliminate all fields in the IPv6 header that can be derived from the 802.15.4 header in the common case
  - Source address : derived from link address
  - Destination address : derived from link address
  - Length : derived from link frame length
  - Traffic Class & Flow Label : zero
  - Next header : UDP, TCP, or ICMP
- UDP Compression
  - Assume common values for header fields and define compact forms

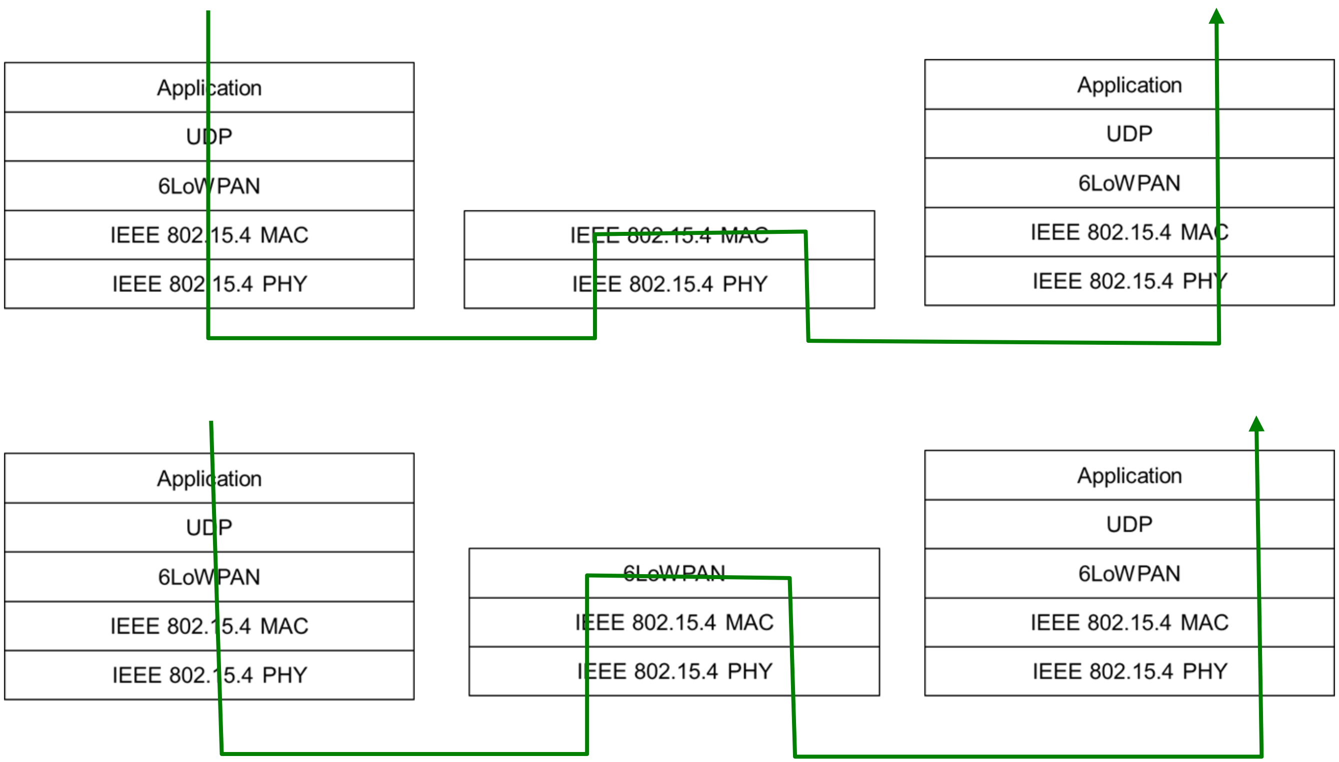
    Ports within 61616 to 61632 (4 bits)

    Length derived from IPv6 Length

    Checksum always carried inline

6LoWPAN: routing modes

- Mesh-under routing
  - Small network
  - L2 forwarding
  - One single IP Subnet
- Route-over routing
  - L3 Routing



6loWPAN: fragmentation and reassembly

- Fragmentation to fit the size of L2 MTU
  - Ethernet 1500 Bytes
  - 802.15.4 127 bytes
  - Wifi 2304 bytes
- Fragment header
  - Tag Value
  - Offset
  - Size
- Mesh-under
  - Fragments are reassembled at destination
- Route-over
  - Fragments are reassembled at every hop

	IPv6 compressed header	
802.15.4 Header	6LoWPAN	Payload

		IPv6 compressed header	
802.15.4 Header	Fragment header	6LoWPAN	Payload

			IPv6 compressed header	
802.15.4 Header	Mesh addr. header	Fragment header	6LoWPAN	Payload

6LoWPAN: a step to 6Lo

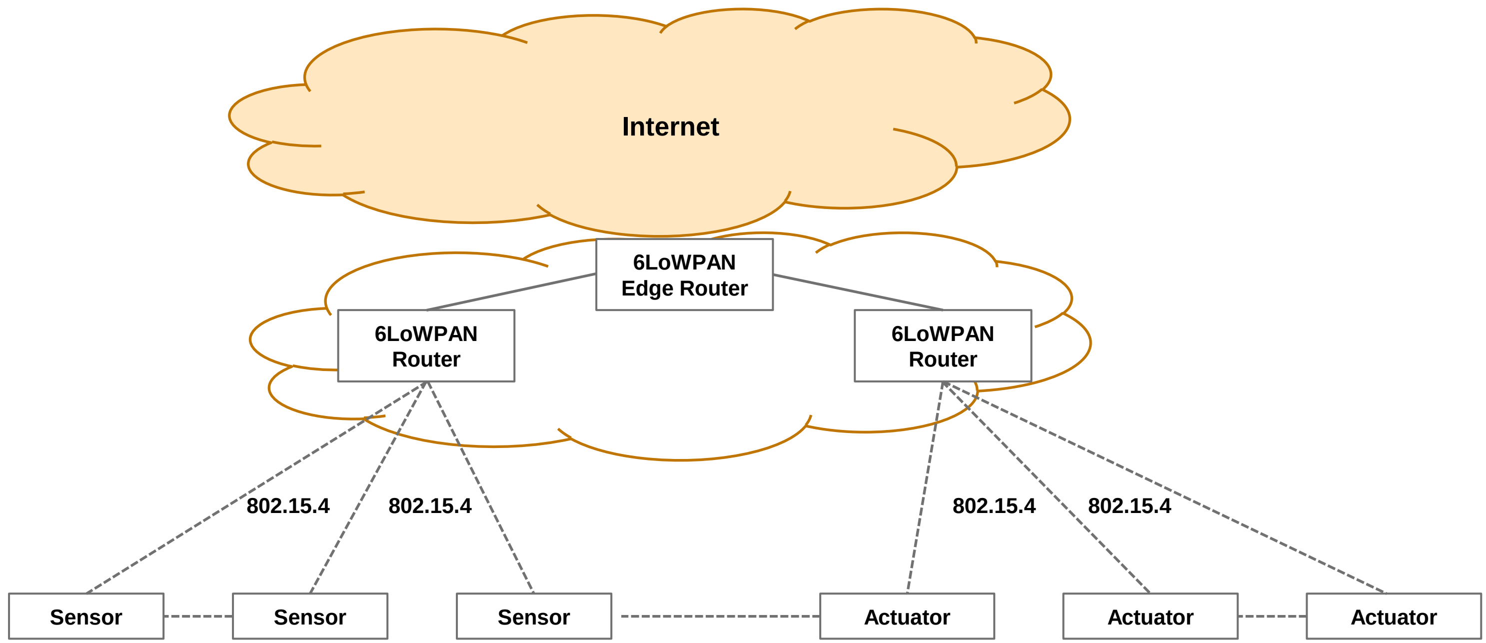
- 6Lo
  - IPv6 over Networks of Resource-constrained Nodes
  - IPv6 over various IoT links
  - Work in progress

IPv6	IPv6	IPv6	IPv6	IPv6
ITU-T G.9959	BLE	802.15.4	NFC	…
RFC 7428	RFC 7668	RFC 7554 RFC 4944	Draft	

- IETF RFC 8480
  - 6TiSCH (Time-Slotted Channel Hopping) Operation Sublayer (6top) Protocol (6P)
- IETF DetNet WG
- IEEE 802.15.4e
  - 6TiSCH WG
- IPv6 Time Slotted Channel Hopping
- Time Sensitive Network
- Time slot structure
- Optimization for Time-Sensitive flows (control loops)
- Scheduling / forwarding

Application
UDP
6LoWPAN 6TISCH (6top)
IEEE 802.15.4 MAC (TSCH)
IEEE 802.15.4 PHY

6loWPAN architecture example



IoT Market

IoT Market: 2030 forecast

- The market is not consolidating (source IoT Analytics)
- Market Value ~ US$ 25 Bn
- CAGR* 2019 – 2030 ~38%
- Connected Devices ~125 Bn (~15 devices / human)
- Revenue 2030 US$ 1,5 Tn
- Industrial/Manufacturing is the #1 vertical (source IoT Analytics)
- It is easy to become an IoT platform company on paper (source IoT Analytics)

* Compound annual growth rate

IoT Market: Plaforms

- Pio
- Arduino
- Arietta G25
- BeagleBoard
- Flutter
- IMUduinoBTLE
- Intel Edison
- Intel Galileo
- LibeliumWaspmote
- LightBlueBean
- Local Motors Connected Car
- Microduino
- Nanode
- OpenKontrolGateway
- OpenPicus
- panStamps
- PicAxe
- Pinoccio
- Raspberry Pi
- RasWIK
- SAM R21 XplainedPro
- SmartEverything
- SODAQ
- SparkFunRedBoard
- Tessel
- Tessel2
- The AirBoard
- The Rascal
- TinyDuino
- UDOO
- WIOT
- XinoRF
- …

IoT Market: 2019 acquisitions

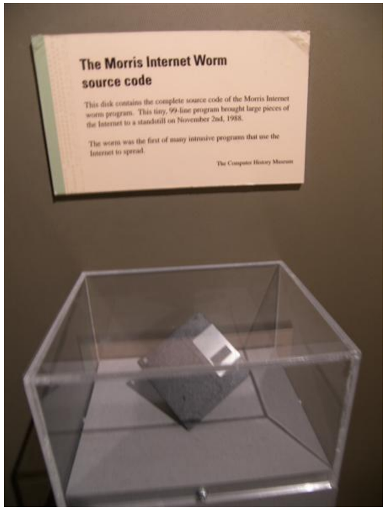
Acquirer	Acquired company	Deal size	Category
Siemens	**Pixeom**	undisclosed	Edge Computing
Aspen Tech	**Mnubo**	$102CAD	Analytics
Vodacom	**IoT.nxt**	undisclosed	IoT Platform
Geotab	**BSM**	undisclosed	Telematics
Digi Intl.	**OpenGear**	$140M	Remote Infrastructure Management
Cisco	**Sentryo**	undisclosed	IoT Security
Microsoft	**Express Logic**	undisclosed	Real-time operating system
Avnet	**Witekio**	undisclosed	Embedded Software
PowerFleet	**Pointer**	$140M	Telematics
Dialog Semiconductor	**Creative Chips**	undisclosed	Semiconductor
Palo Alto Networks	**Zingbox**	$75M	IoT Security
Cognizant	**Zenith Technologies**	undisclosed	IoT System Integration in Life Sciences

Source: IoT Analytics

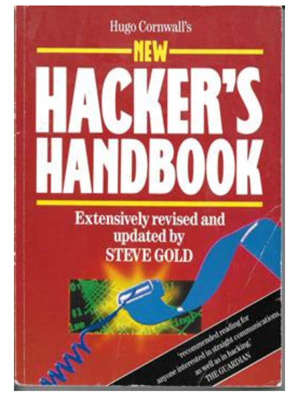
IoT Market: Cloud competitors

- AWS IoT
- ThingSpeak
- Samsung ARTIK™ Cloud
- Microsoft Azure IoT Platform
- IBM Watson IoT™

IoT Security



The Morris Internet Worm
source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intrusive programs that use the Internet to spread.
The Computer History Museum



Hugo Cornwall's
NEW
HACKER'S
HANDBOOK
Extensively revised and updated by
STEVE GOLD

CAP'N CRUNCH

IoT Security: Awareness and obviousness

- Threats vs risks or objectivity vs subjectivity
- Expertise in IoT security must begin with an expertise in networks
- A counter measure may have security vulnerabilities !
- No absolute security
- Countermeasures evolve … threats too
- Computer abuse is illegal in networking, thus punished by the law …

- Law « Informatique et libertés » of 1978
  - First law in the TIC domain

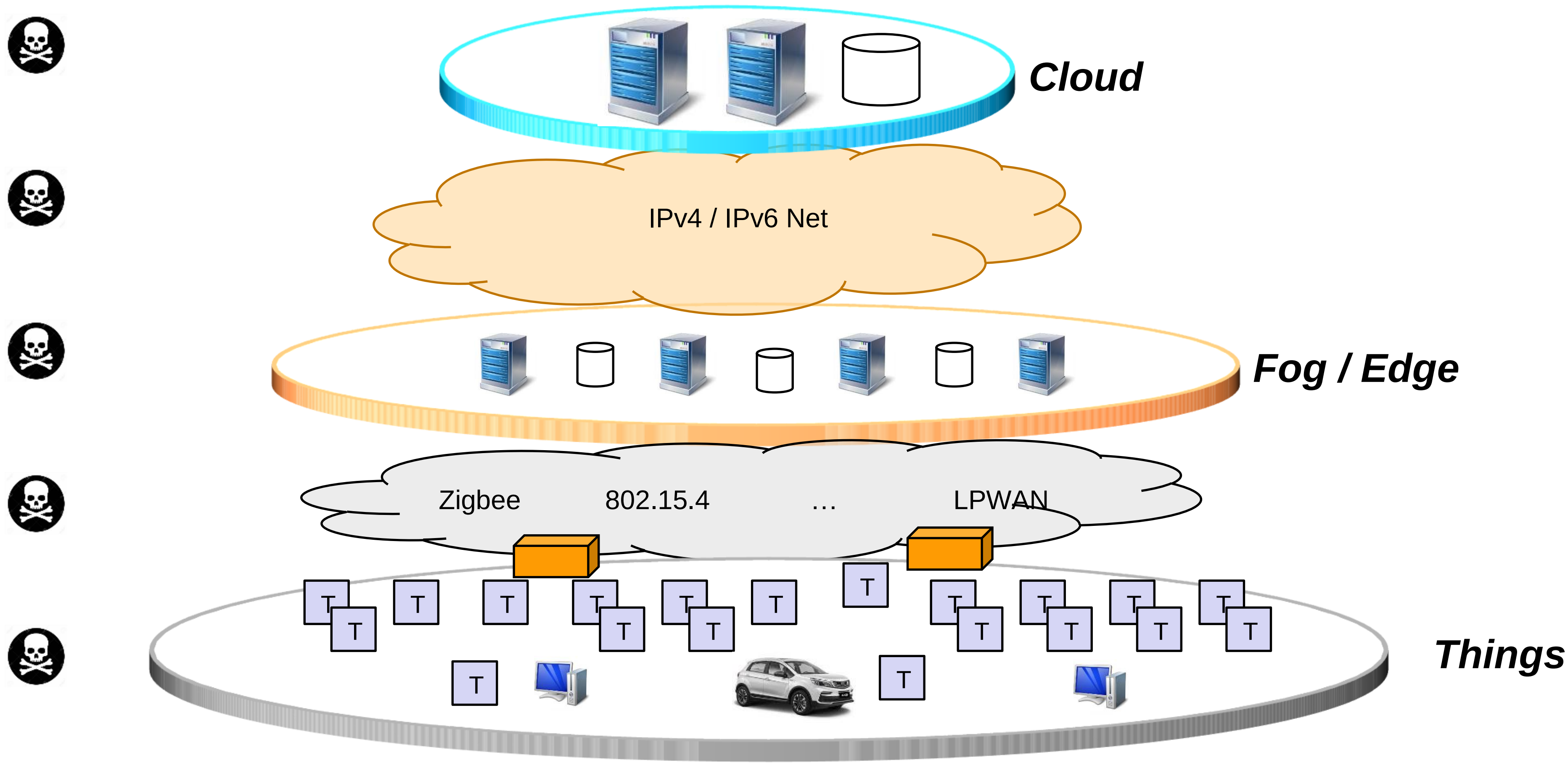
- Law 88-19 of 1988 aka “GODFRAIN law”.
  - Aim to sanction delinquency in computing.
  - First law of this kind in France.
  - 3 years imprisonment / 45 000 € fine

- Law 2004-575 called LCEN « Loi de Confiance sur l’Economie Numérique »
  - Published in the Official Journal n°143 22 June 2004
  - Clarify the rights and duties of actors
  - Set a frame for e-trading
  - 5 years imprisonment / 75000 Euros fine

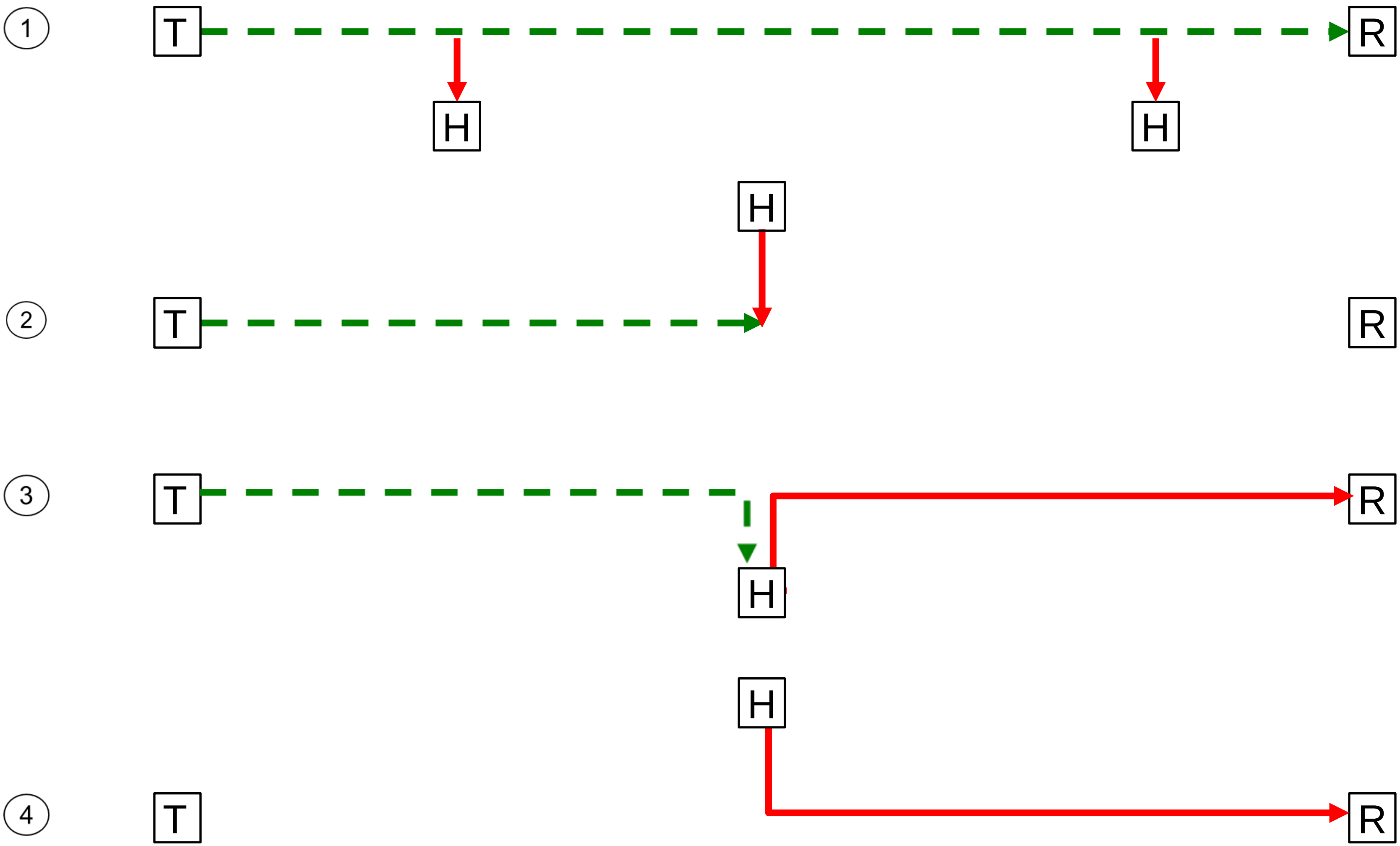
- Law 2013-1168 published on the 18 December 2013 aka LPM
  - Military programming law containing various provisions concerning defense and national security

- *Law 2018-493 published on the 20 June 2018 modified the 1978 law to ensure conformity with the national and European law.
  - Allow to concretely apply the General Rules on Data Protection (RGPD) and the « Police-justice » directive about criminal files.

- Huge attack surface
- Lack of security SW within IoT Devices
- IoT manufacturers aware of?
- Thousand unsecure IoT deployed
- Things used for DDoS
- Unencrypted flow by default
- Coding errors
- Buffer overflow
- Clear text protocols
- Unnecessary open ports
- Etc. …

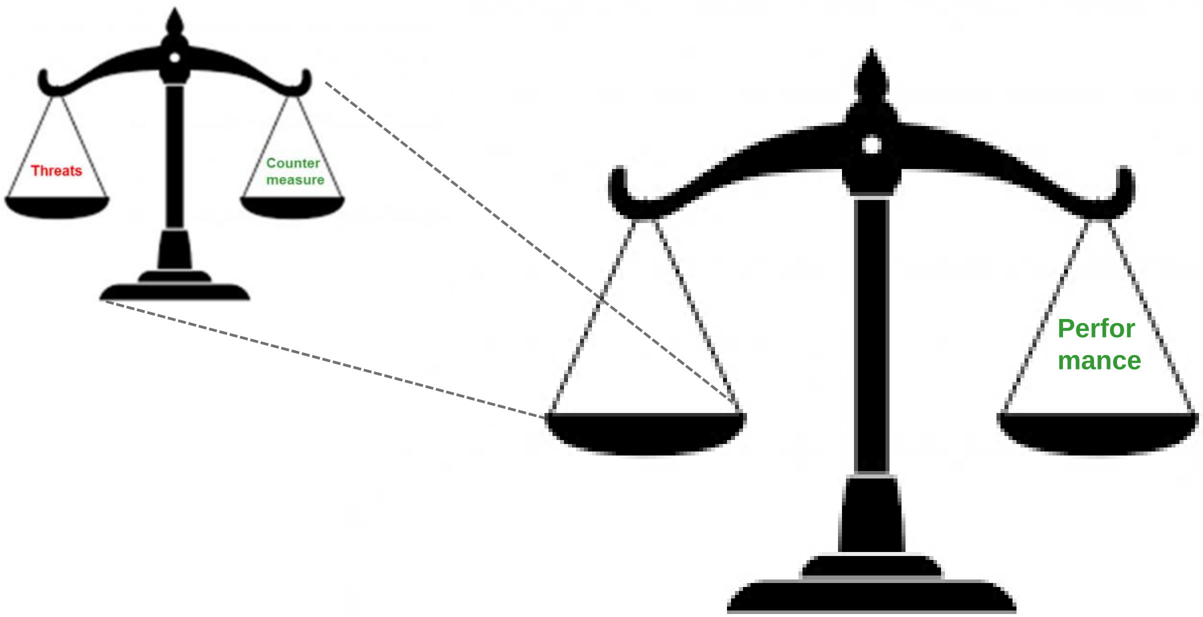

Cloud
IPv4 / IPv6 Net
Fog / Edge
Zigbee
802.15.4
…
LPWAN
T
Things

IoT Security: threats on IoT flows

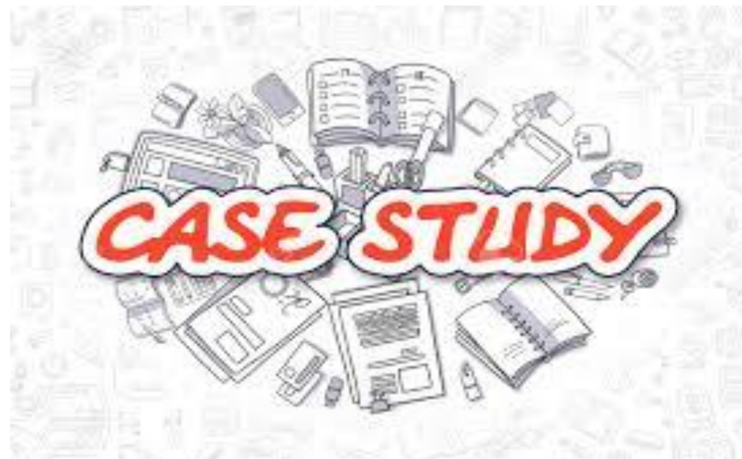


- IoT Flows encryption
- Secured Protocols
- Secured Edge Architecture
- Stakeholders' awareness
- Security norms & standards
- …

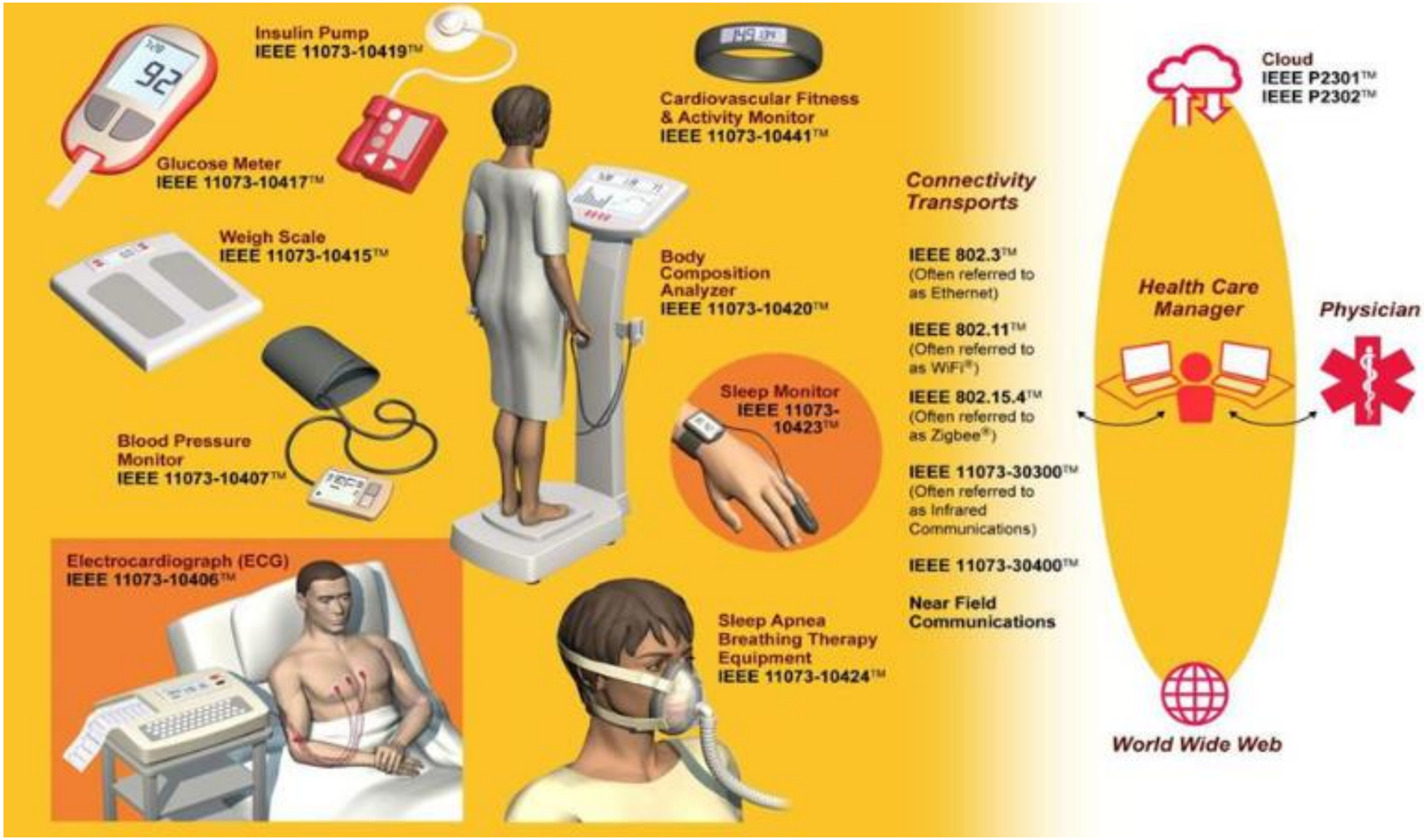
- Threats & Countermeasures mustn't impact performance !



Case Study

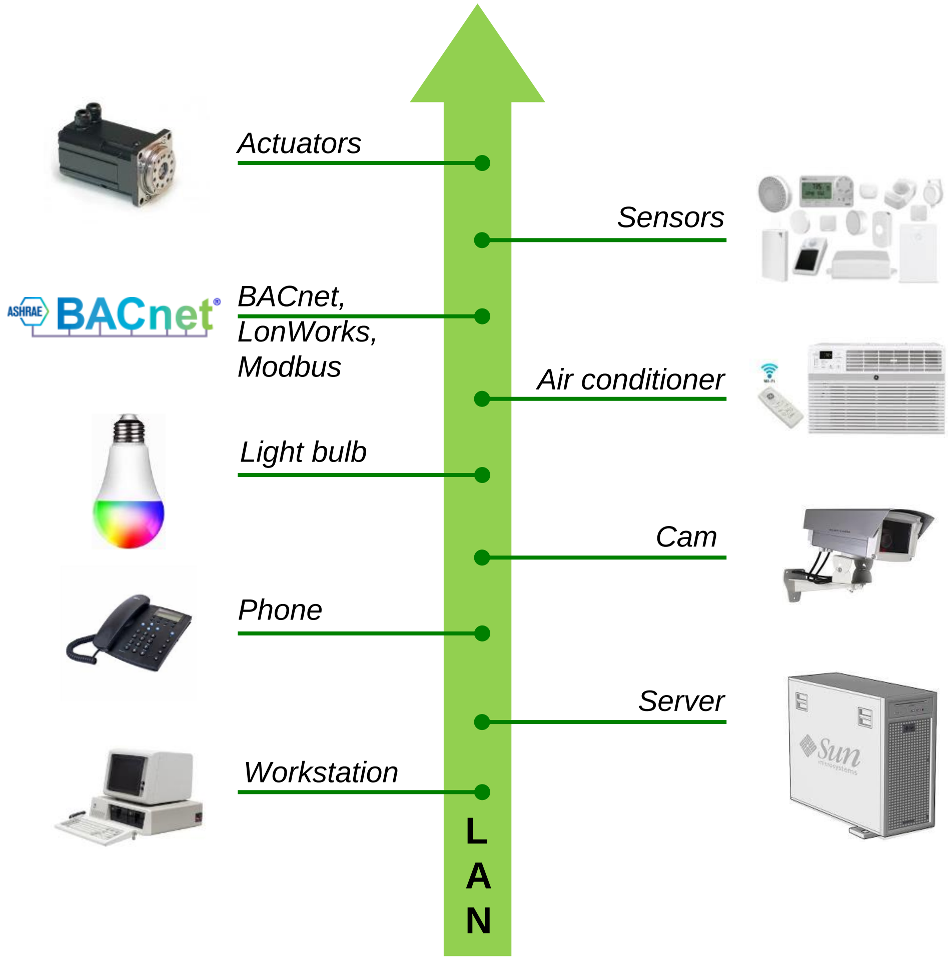


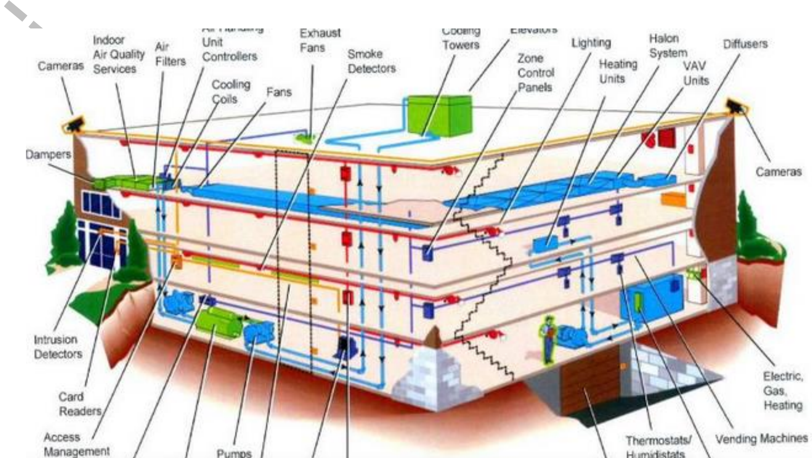
- Log information
- Reduces assembly time
- Augmented Reality driven instructional
- Predictive maintenance


Insulin Pump
IEEE 11073-10419™
Glucose Meter
IEEE 11073-10417™
Weigh Scale
IEEE 11073-10415™
Blood Pressure Monitor
IEEE 11073-10407™
Electrocardiograph (ECG)
IEEE 11073-10406™
Cardiovascular Fitness & Activity Monitor
IEEE 11073-10441™
Body Composition Analyzer
IEEE 11073-10420™
Sleep Monitor
IEEE 11073-10423™
Sleep Apnea Breathing Therapy Equipment
IEEE 11073-10424™
Connectivity Transports
IEEE 802.3™
(Often referred to as Ethernet)
IEEE 802.11™
(Often referred to as WiFi®)
IEEE 802.15.4™
(Often referred to as Zigbee®)
IEEE 11073-30300™
(Often referred to as Infrared Communications)
IEEE 11073-30400™
Near Field Communications
Cloud
IEEE P2301™
IEEE P2302™
Health Care Manager
Physician
World Wide Web

Source: IEEE

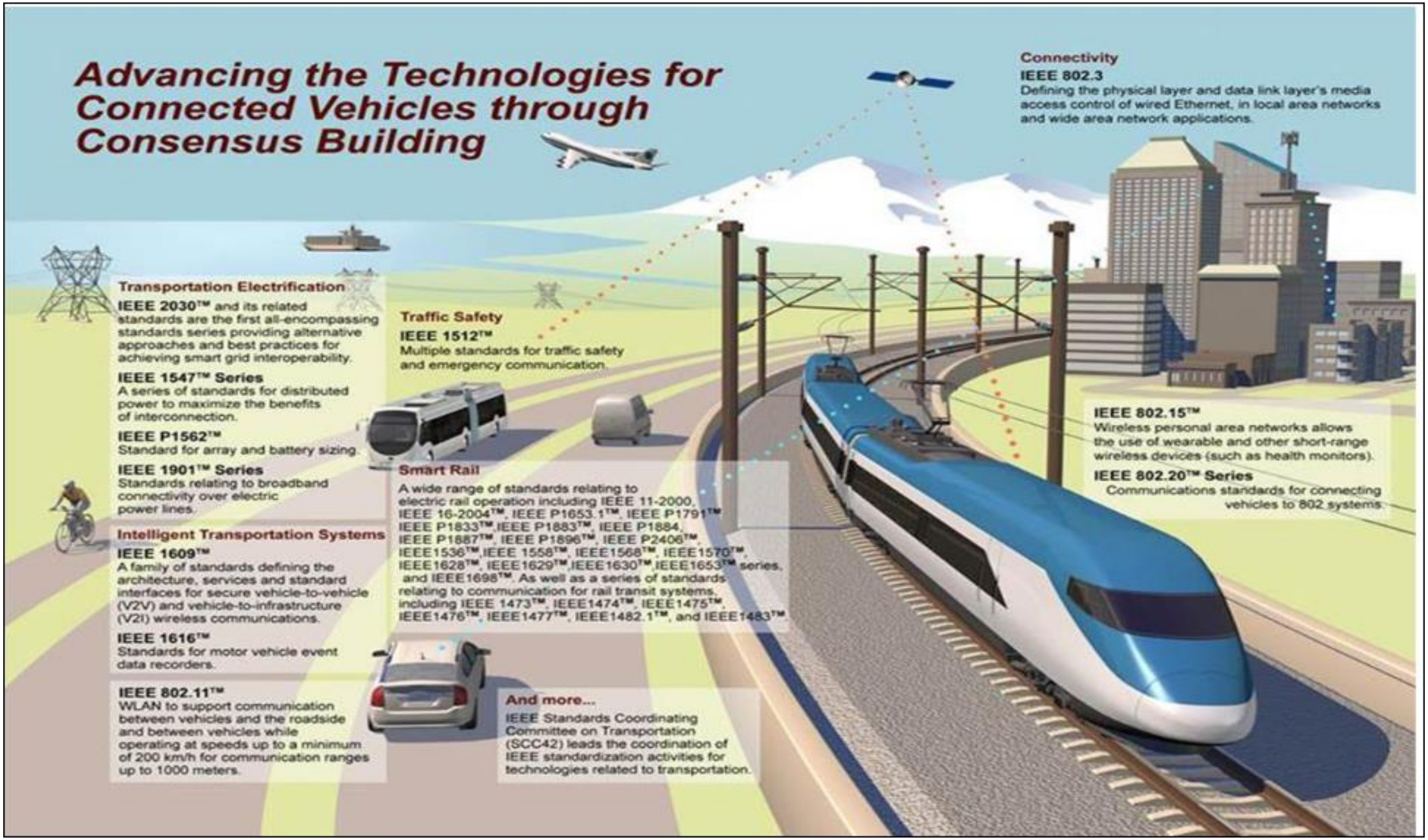
- The LAN to support all usage
- From many dedicated infrastructure/network to a shared network





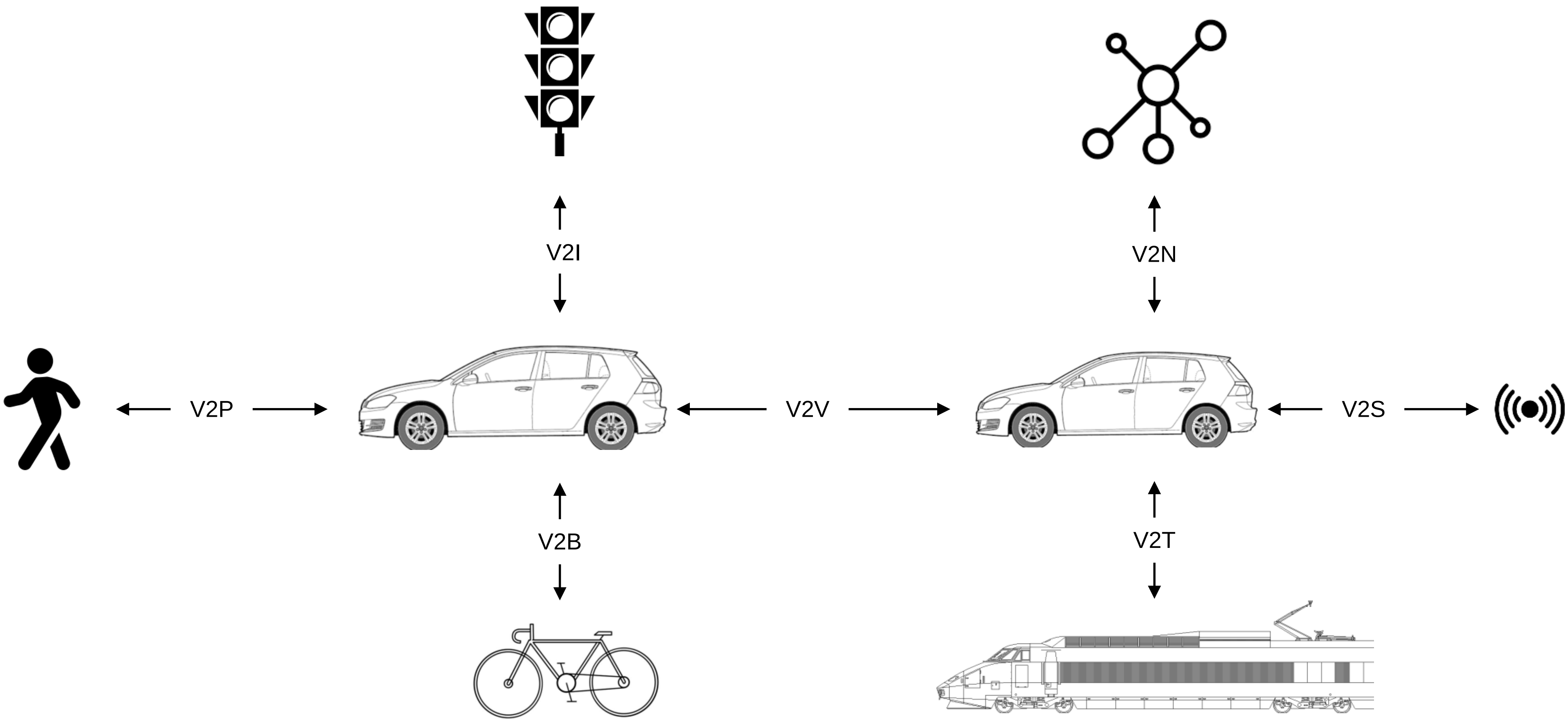
Source Cisco

Smart Transportation



Source: IEEE

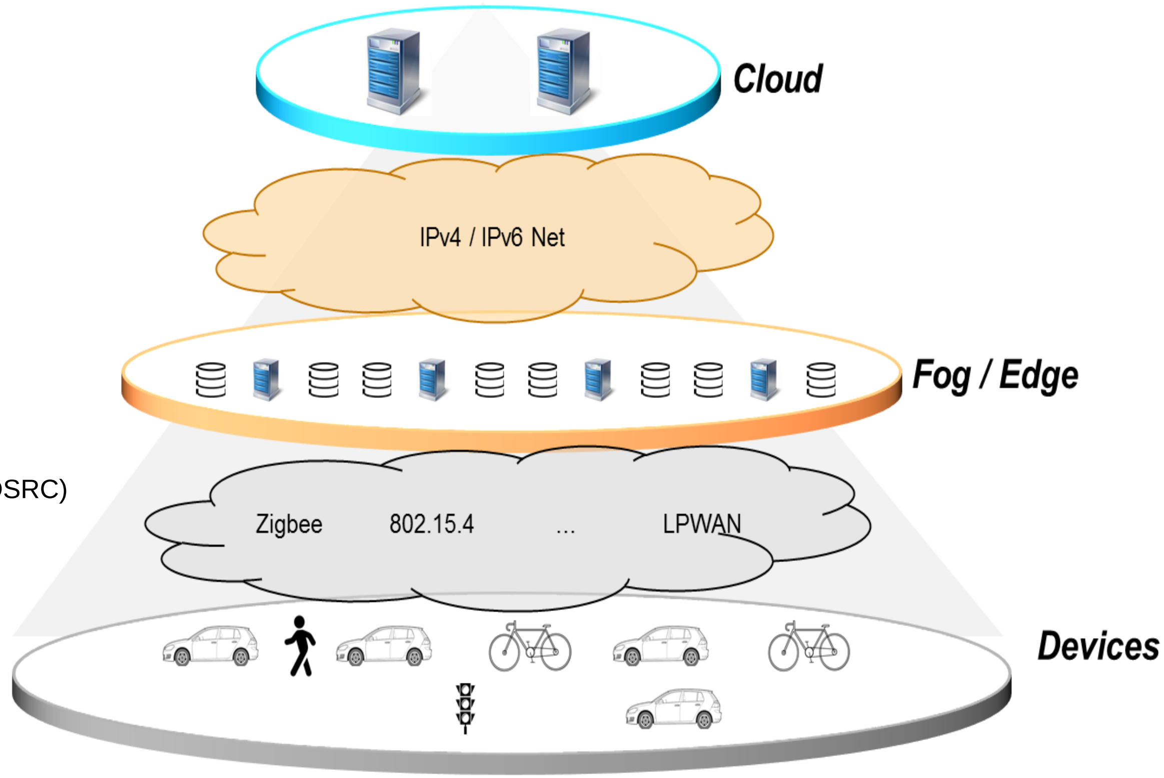
Smart vehicles: V2X



- Multi-access edge computing (MEC
- Vehicle as edge?

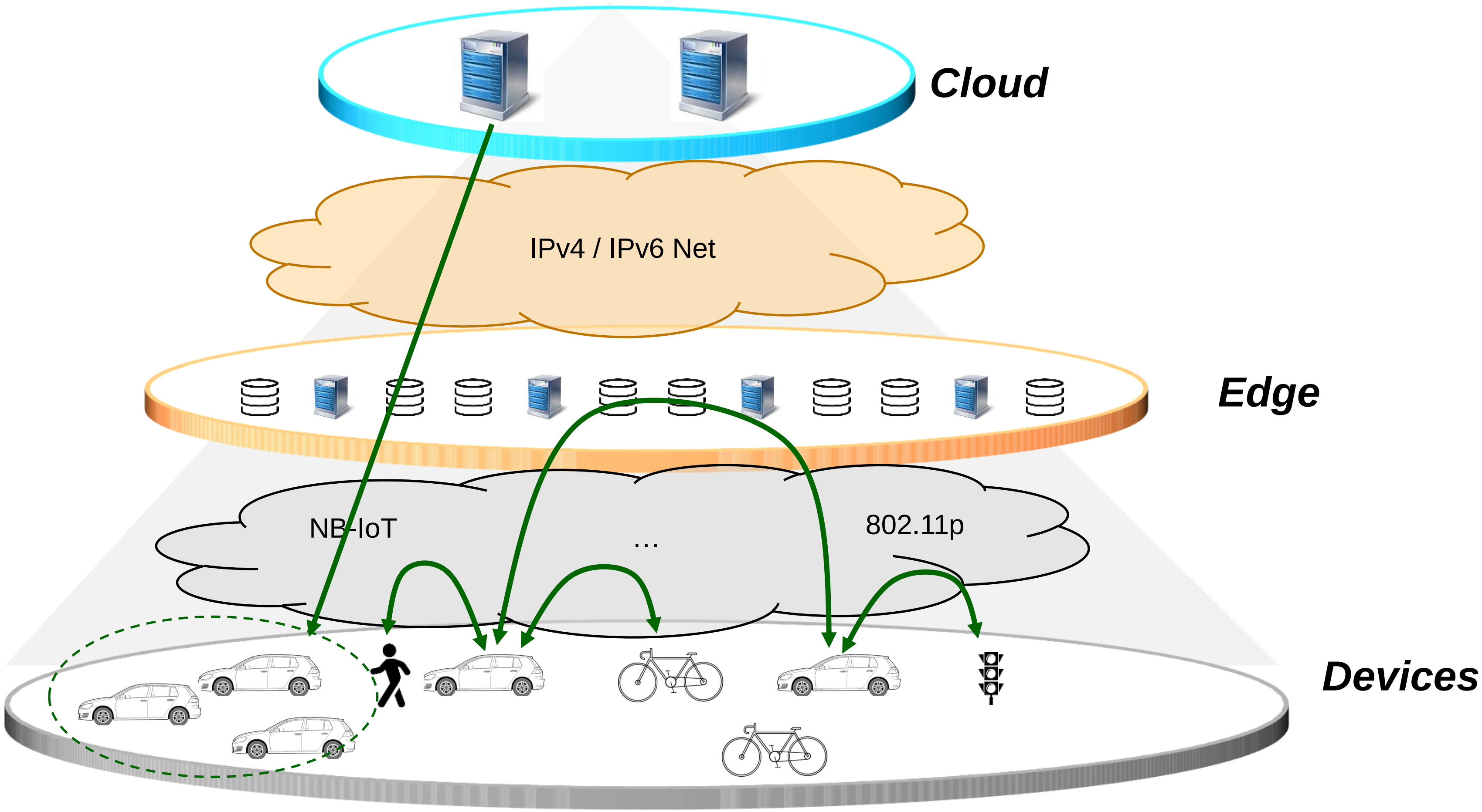
- (Dedicated Short-Range Communications (DSRC)
- 802.11p to support DSRC app.
- LTE-V2X
- …

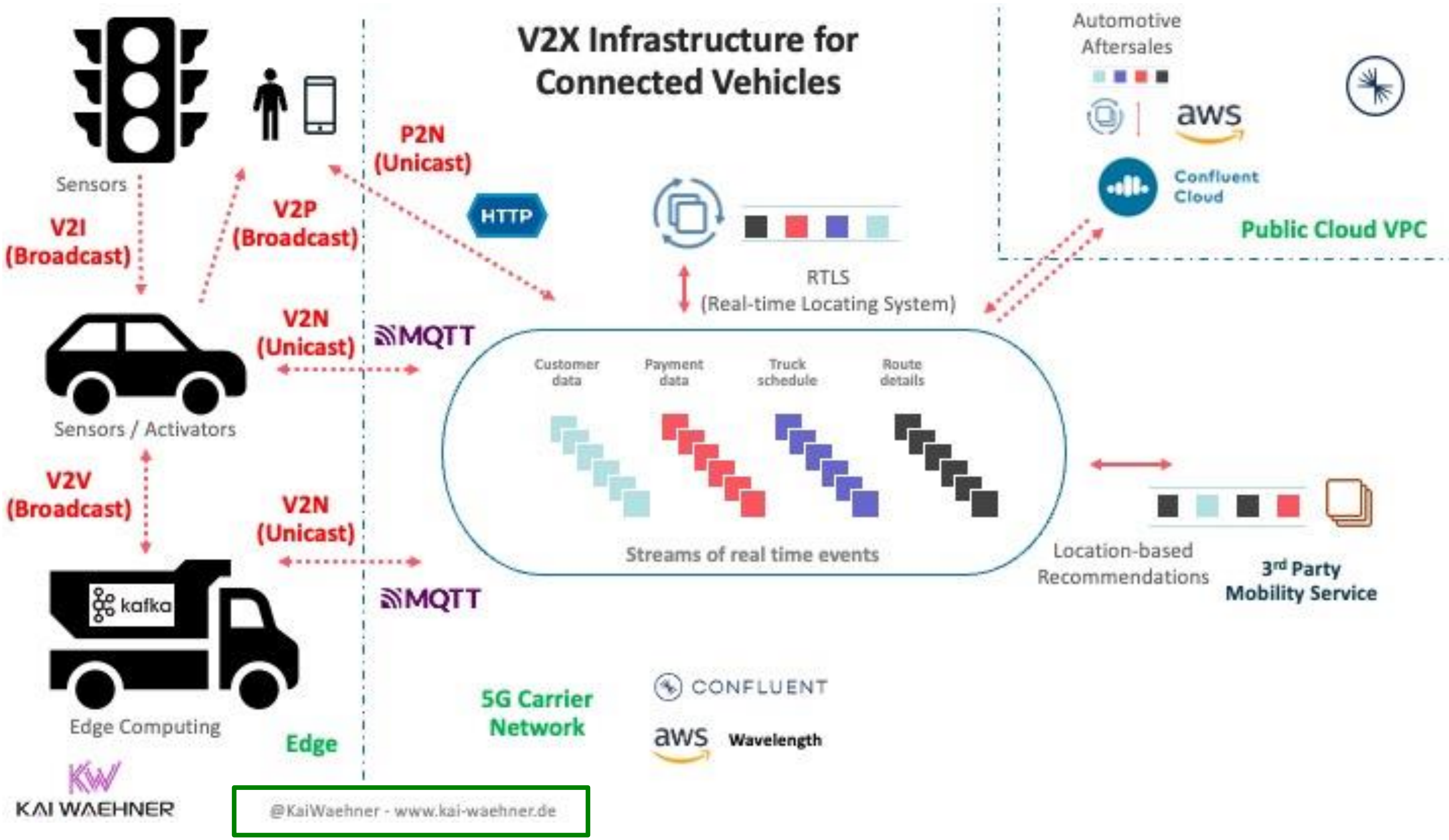
- Roadside Unit (RSU)
- Vehicle as Edge
- Car fist or infrastructure first?



- VRU safe interaction
- Vehicles platooning
- Advanced driving
- Remote driving

- Periodic message (beacon)
- Local event triggered message
- Global event triggered message
- Emergency vehicle message


Cloud
IPv4 / IPv6 Net
Edge
NB-IoT
...
802.11p
Devices



V2X Infrastructure for Connected Vehicles
Sensors
V2I (Broadcast)
V2P (Broadcast)
P2N (Unicast)
HTTP
Sensors / Activators
V2N (Unicast)
MQTT
V2V (Broadcast)
V2N (Unicast)
MQTT
kafka
Edge Computing
Edge
KAI WAEHNER
5G Carrier Network
CONFLUENT
aws Wavelength
RTLS (Real-time Locating System)
Customer data
Payment data
Truck schedule
Route details
Streams of real time events
Automotive Aftersales
aws
Confluent Cloud
Public Cloud VPC
Location-based Recommendations
3rd Party Mobility Service
@KaiWaehner - www.kai-waehner.de

- V2I Safety
- V2V Safety
- Mobility
- Smart roadside
- Environnent
- …

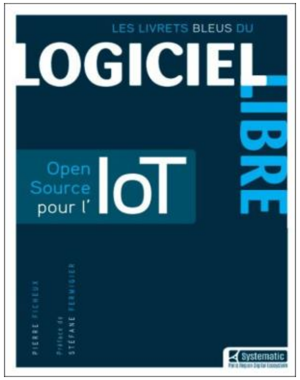
- Data ownership / rights
- Dynamic decisions
- Consumer awareness
- Privacy
- Cybersecurity
- Liability (AI, health , …)
- Curacy
- Business model
- Oligopolies
- Fairness
- e-waste
- …

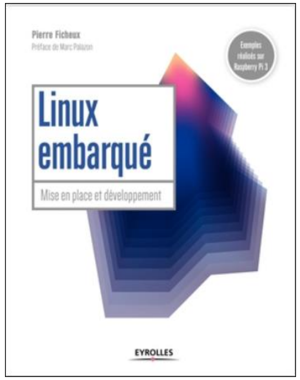
From source: Dr. Shoumen Datta of Massachusetts Institute of Technology (MIT)

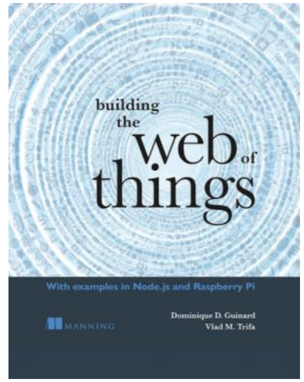
References

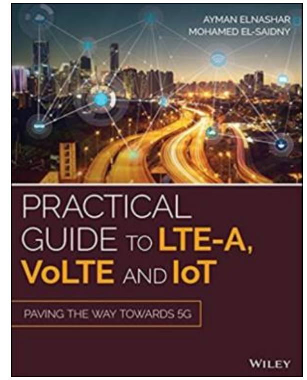
- http://www.utsystem.edu/offices/board-regents/uts165-standards
- https://securityintelligence.com/the-importance-of-ipv6-and-the-internet-of-things/
- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx
- https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf
- https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf
- http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html
- http://blog.trendmicro.com/trendlabs-security-intelligence/high-profile-mobile-apps-at-risk-due-to-three-year-old-vulnerability/#
- http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about
- https://thenewstack.io/tutorial-prototyping-a-sensor-node-and-iot-gateway-with-arduino-and-raspberry-pi-part-1
- http://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf
- http://blog.talosintel.com/2016/02/trane-iot.html
- http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/
- http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/
- …

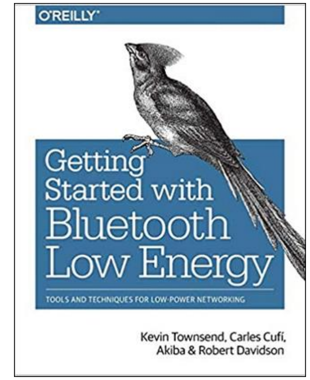
References

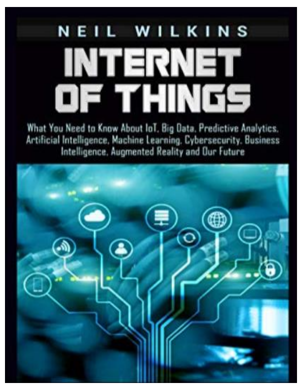


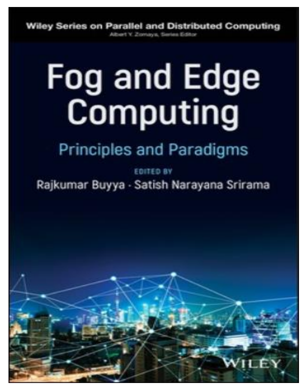












Many more …

Q & A

Exercises